

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-152196

(43)Date of publication of application : 24.05.2002

(51)Int.Cl. H04L 9/32
G09C 1/00
H04Q 7/38

(21)Application number : 2001-250922

(71)Applicant : NEC CORP

(22)Date of filing : 22.08.2001

(72)Inventor : ICHISE NORIYOSHI

(30)Priority

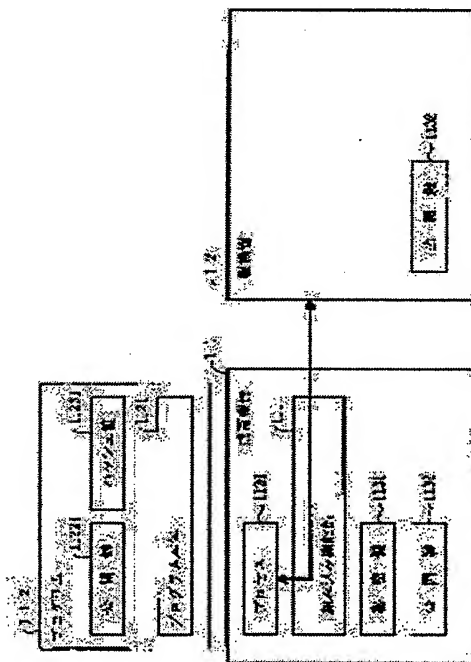
Priority number : 2000264850 Priority date : 01.09.2000 Priority country : JP

(54) METHOD FOR PROGRAM AUTHENTICATION WITHOUT SECRET KEY, PROGRAM ID COMMUNICATION PROCESSING CONTROL METHOD, PROGRAM ID COMMUNICATION RANGE CONTROL METHOD, AND METHOD FOR PROVIDING COMMUNICATION LINE BY OPEN KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent personation of communication in an environment wherein readout and forgery are allowed.

SOLUTION: Portable equipment 11 confirms by a built-in function part 111 that a hash value 11231 is generated by a program main body 1121 and a secret key paired with an open key 11221 indicating the origin of a program 112. Master equipment 12 authenticates the portable equipment 11 by an open key system which uses an open key 11232 and the secret key 1131 and then decides whether or not the program 112 has the authentic origin according to the hash value confirmation result of the portable equipment 11 when the authentication is successful. When the master equipment 12 successfully authenticates the portable equipment 11 and the program 112 has the authentic origin, it is considered that the program 112 is authenticated with the open key 11221.



LEGAL STATUS

[Date of request for examination] 22.08.2001

[Date of sending the examiner's decision of rejection] 01.12.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

*** NOTICES ***

JPO and NCIPJ are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key showing the source origin of this program and the signature performed to said program body with this public key and the private key which makes a pair are included. The process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When it is able to be checked that said signature is generated with the public key showing the source origin of said program body and said program and the private key which makes a pair The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, The private-key-less program authentication approach characterized by including the process which said communication link and processor attest with expressing the source origin of said program for this public key when the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained.

[Claim 2] In the process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair Said signature consists of a signature value enciphered with the public key which expresses the source origin of said program for the digest which carried out hashing of said program body by the Hash Function, and the private key which makes a pair. While said program execution and communication device decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program body by the Hash Function, and a digest is obtained. The private-key-less program authentication approach according to claim 1 characterized by judging whether both digests are in agreement.

[Claim 3] In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device It judges whether the public key in which said communication link and processor equip with the public key in which the partner who may communicate is shown, and the partner who may this communicate is shown,

and the public key which accompanies said program execution and communication device are in agreement. The private-key-less program authentication approach according to claim 1 or 2 characterized by attesting said program execution and communication device when in agreement.

[Claim 4] In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor The private-key-less program authentication approach according to claim 1 or 2 which will be characterized by attesting said program execution and communication device if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 5] In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key group showing the source origin of this program and the signature group performed with each public key and each private key which makes a pair to the data created combining said program body and said public key group are included. It checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair. The process which obtains the assembly of the public key corresponding to the signature by which being generated was checked, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained The private-key-less program authentication approach characterized by including the process at which said communication link and processor attest each public key of the signature check result by said program execution and communication device with expressing the source origin of said program.

[Claim 6] It checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair. In the process which obtains the assembly of the public key corresponding to the checked signature Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created in the combination of said program body and said public key group by the Hash Function, and each private key which makes a pair. Said program execution and communication device Carry out hashing of the data created in the combination of said program body and said public

key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by the Hash Function, and a digest is obtained. The private-key-less program authentication approach according to claim 5 characterized by judging whether this digest and said digest group are in agreement.

[Claim 7] In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device It judges whether the public key in which said communication link and processor equip with the public key in which the partner who may communicate is shown, and the partner who may this communicate is shown, and the public key which accompanies said program execution and communication device are in agreement. The private-key-less program authentication approach according to claim 5 or 6 characterized by attesting said program execution and communication device when in agreement.

[Claim 8] In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor The private-key-less program authentication approach according to claim 5 or 6 which will be characterized by attesting said program execution and communication device if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 9] In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device Said program contains the program body and ID group showing the source origin of this program. Said program execution and communication device include the process generated and performed based on said program. Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program When the process which obtains a part or all of ID group to which said communication link and processor express the source origin of the program which becomes the origin of said process, and one or more ID showing said source origin are obtained In the process at which said communication link and processor communicate with said program execution and communication device by processing of the process generated based on said program, and the processing generated by communication link The program ID communications processing control approach characterized by including the process which performs the access control carried out based on ID group to which said communication link and processor express said source origin obtained from said program execution and management equipment.

[Claim 10] In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device Said program contains the program body, the public key showing the source origin of this program, and this public key and the private key which makes a pair. Said program execution and communication device include the process generated and performed based on said program. Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process which obtains the public key showing the source origin of said program which said communication link and processor become from said program execution and communication device the origin of the process which makes this program execution and

communication device communicate, When said program is attested with the process which attests said program with the public key system using the public key and private key with which said communication link and processor express the source origin of said program The program ID communications processing control approach characterized by including the process at which said communication link and processor communicate with said program execution and communication device by the access control carried out based on said public key.

[Claim 11] In the process which attests said program with the public key system using the public key and private key with which said communication link and processor express the source origin of said program about the obtained public key The one-time password method by the public key is used. Said program execution and communication device Delivery, and said communication link and processor a character string random to said program execution and communication device to said communication link and processor for said public key Delivery, The character string as which said program execution and communication device enciphered this character string with said private key is returned to said communication link and processor. The program ID communications processing control approach according to claim 10 which will be characterized by attesting said program if the character string which said communication link and processor decoded the enciphered character string with said sent public key, and decoded, and the character string sent previously are in agreement.

[Claim 12] In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key showing the source origin of this program and the signature performed to said program body with this public key and the private key which makes a pair are included. The process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When it is able to be checked that said signature is generated with the public key showing the source origin of said program body and said program and the private key which makes a pair The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained The program ID communications processing control approach characterized by including the process which communicates with said program execution and communication device by the access control which said communication link and processor obtained the public key showing the source origin of said program from said program execution and communication device, and carried out based on this public key.

[Claim 13] In the process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair Said signature consists of a signature value enciphered with the public key which expresses the source origin of said program for the digest which carried out hashing of said program body by the Hash Function, and the private key which makes a pair. While said program execution and communication device decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program body by the Hash Function, and a digest is obtained. The program ID communications processing control approach

according to claim 12 characterized by judging whether both digests are in agreement.

[Claim 14] The program ID communications-processing control approach according to claim 12 or 13 characterized by to judge that the public key with which said communication link and processor is equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication device in the process with which said communication link and processor attests said program execution and communication device with the public key system using the public key and the private key which accompanies said program execution and communication device, and the public key in which said partner who may communicate is shown are in agreement.

[Claim 15] In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor The program ID communications processing control approach according to claim 12 or 13 which will be characterized by attesting said program execution and communication device if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 16] In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key group showing the source origin of this program and the signature group performed with each public key and each private key which makes a pair to the data created combining said program body and said public key group are included. It checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair. The process which obtains the assembly of the public key corresponding to the signature by which being generated was checked, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained The program ID communications processing control approach characterized by including the process which communicates with said program execution and communication device by the access control which said communication link and processor carried out based on a part or all of an assembly of a public key by said program execution and communication device. [of a signature check result]

[Claim 17] In the process which checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each

private key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program body and said public key group by the Hash Function, and each private key which makes a pair. Said program execution and communication device Each digest which decoded each signature value with each public key, respectively, The program ID communications processing control approach according to claim 16 characterized by judging whether the digest obtained by carrying out hashing of the data created combining said program body and said public key group by the Hash Function is in agreement.

[Claim 18] The program ID communications-processing control approach according to claim 16 or 17 characterized by to judge that the public key with which said communication link and processor is equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication device in the process with which said communication link and processor attests said program execution and communication device with the public key system using the public key and the private key which accompanies said program execution and communication device, and the public key in which said partner who may communicate is shown are in agreement.

[Claim 19] In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor The program ID communications processing control approach according to claim 16 or 17 which will be characterized by attesting said program execution and communication device if it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement.

[Claim 20] In the information system constituted by the program, and two or more program executions and communication devices which generate a process, respectively and perform it based on these programs Said program contains the program body and ID group showing the source origin of this program. A certain process which the program execution and the communication device which exists based on a certain program generated Before communicating with a certain another process to which another a certain program execution and communication device generated this program or a certain another program to origin When ID group which expresses said source origin as the process which obtains a part or all of ID group to which both program executions and a communication device express the source origin of said program which becomes the origin of the process in partner program execution and a communication device is obtained ID group showing the source origin of said program which becomes ID group to which both program executions and a communication device express the obtained source origin, and the origin of the process in self-program execution and a communication device is compared. The program ID communication link range control approach characterized by including the process which will open a channel if one or more ID showing the source origin of said program in agreement exists.

[Claim 21] In the information system constituted by the program, and two or more program executions and communication devices which generate and perform each process based on each program Said program contains the program body, the public key showing the source origin of this program, and this public key and the private key which makes a pair. A certain process which the program execution and the communication device which exists based on a certain program generated Before communicating with a certain another process to which another a certain program execution and communication device generated this program or a certain another program to origin The process which obtains the public key with which both program executions and a communication device express the source origin of said program which

consists of partner program execution and a communication device the origin of the process in partner program execution and a communication device, respectively, The process which judges whether the public key showing the source origin of said program which both program executions and a communication device become the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement, The process which performs mutual recognition of the program which both program executions and a communication device become the origin of the process in partner program execution and a communication device using the public key and private key showing the source origin of said program which becomes the origin of the process in partner program execution and a communication device, The public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement. And the program ID communication link range control approach characterized by both program executions and a communication device including the process which opens a channel when mutual recognition of the program which becomes the origin of the process in partner program execution and a communication device is carried out.

[Claim 22] In the process which performs mutual recognition of the program which both program executions and a communication device become the origin of the process in partner program execution and a communication device using the public key and private key showing the source origin of said program which becomes the origin of the process in partner program execution and a communication device The one-time password method by the public key is used. Both program executions and a communication device The public key which accompanies self-program execution and a communication device to partner program execution and a communication device Delivery, A random character string to partner program execution and a communication device, respectively Delivery, The character string enciphered with the public key with which partner program execution and a communication device express the source origin of said program which becomes the origin of the process in partner program execution and a communication device about this character string, and the private key which makes a pair is returned to self-program execution and a communication device. If self-program execution and a communication device decode the enciphered character string with a corresponding public key and the decoded character string and the character string sent previously are in agreement The program ID communication link range control approach according to claim 21 characterized by attesting the program which becomes the origin of the process in partner program execution and a communication device communication device.

[Claim 23] In the information system constituted by the program, and two or more program executions and communication devices which generate and perform each process based on each program The public key and private key with which said program execution and communication device accompany self-program execution and a communication device, The public key which accompanies partner program execution and a communication device, and the process generated and performed based on said program are included. Said program The program body, The public key showing the source origin of this program and the signature performed to said program body with this public key and the private key which makes a pair are included. A certain process which the program execution and the communication device which exists based on a certain program generated Before communicating with a certain another process to which another a certain program execution and communication device generated this program or a certain another program to origin The process which checks whether both program executions and a communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair, The process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device before performing said communication link, When it is able to be checked that both program executions and a communication device are generated with the public key with which said signature expresses the source origin of said program body and said program, and the private key which

makes a pair The process which transmits said public key to partner program execution and a communication device before performing said communication link, The process which judges whether the public key showing the source origin of said program which both program executions and a communication device become the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement, Mutual recognition of the program which becomes the origin of the process in partner program execution and a communication device is carried out. And when the public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement The program ID communication link range control approach characterized by both program executions and a communication device including the process which opens a channel.

[Claim 24] In the process which checks whether both program executions and a communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair Said signature consists of a signature value enciphered with the public key which expresses the source origin of said program for the digest which carried out hashing of said program body by the Hash Function, and the private key which makes a pair. While both program executions and a communication device decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program body by the Hash Function, and a digest is obtained. The program ID communication link range control approach according to claim 23 or 24 characterized by judging whether both digests are in agreement.

[Claim 25] In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device Both program executions and a communication device are equipped with the public key in which the partner who may communicate is shown. The program ID communication link range control approach according to claim 23 or 24 characterized by judging whether the public key in which the this partner who may communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication device are in agreement.

[Claim 26] In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device The one-time password method by the public key is used. Self-program execution and a communication device The public key which accompanies partner program execution and a communication device is obtained from partner program execution and a communication device. A random character string to partner program execution and a communication device delivery, and partner program execution and a communication device This character string is enciphered with the private key which accompanies partner program execution and a communication device, and it returns to self-program execution and a communication device. Self-program execution and a communication device The program ID communication link range control approach according to claim 23 or 24 which will be characterized by attesting partner program execution and a communication device if it decodes with said public key which obtained the enciphered character string from partner program execution and a communication device and the decoded character string and the character string sent previously are in agreement.

[Claim 27] When there is a public key both program executions and a communication device succeed in authentication of partner program execution and a communication device, and corresponds with the assembly of the public key of the signature check result by both program executions and the communication device The communication device with which both program executions and a communication device form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key,

When the public key showing the source origin of said program is obtained including the resource group for channels In case the process generated based on said program communicates, the communication device of both program executions and a communication device The program ID communication link range control approach according to claim 26 characterized by assigning a channel resource to one of the virtual channel resource groups corresponding to the public key showing the obtained source origin, and offering a channel using a virtual channel resource.

[Claim 28] In the information system constituted by the program, and two or more program executions and communication devices which generate and perform each process based on each program The public key and private key with which said program execution and communication device accompany self-program execution and a communication device, The public key which accompanies partner program execution and a communication device, and the process generated and performed based on each program are included. Each program The program body, The public key group showing the source origin of this program and the signature group performed with each public key and each private key which makes a pair to the data created combining said program body and said public key group are included. The process which checks whether both program executions and a communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair, and both program executions and a communication device The process which attests partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device, Both program executions and a communication device tell the assembly of the public key of the signature check result by self-program execution and the communication device to partner program execution and a communication device. The process which judges whether there is any public key which is in agreement with the assembly of the public key of the signature check result by self-program execution and the communication device and the assembly of the public key of the signature check result by partner program execution and the communication device, One or more public keys which succeed in authentication of partner program execution and a communication device, and are in agreement with the assembly of the public key of the signature check result by both program executions and the communication device at a certain time The program ID communication link range control approach characterized by both program executions and a communication device including the process which opens the channel between processes.

[Claim 29] In the process which judges whether both program executions and a communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program body and said public key group by the Hash Function, and each private key which makes a pair. Partner program execution and a communication device Carry out hashing of the data created by said program body and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by the Hash Function, and a digest is obtained. The program ID communication link range control approach according to claim 28 characterized by judging whether this digest and said digest group are in agreement.

[Claim 30] In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device Both program executions and a communication device are equipped with the public key in which the partner who may communicate is shown. The program ID communication link range control approach according to claim 28 or 29 characterized by judging whether the public key in which the this partner who may communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication device are in agreement.

[Claim 31] In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device The one-time password method by the public key is used. Self-program execution and a communication device The public key which accompanies partner program execution and a communication device is obtained from partner program execution and a communication device. A random character string to partner program execution and a communication device delivery, and partner program execution and a communication device This character string is enciphered with the private key which accompanies partner program execution and a communication device, and it returns to self-program execution and a communication device. Self-program execution and a communication device The program ID communication link range control approach according to claim 28 or 29 which will be characterized by attesting partner program execution and a communication device if it decodes with said public key which obtained the enciphered character string from partner program execution and a communication device and the decoded character string and the character string sent previously are in agreement.

[Claim 32] When there is a public key both program executions and a communication device succeed in authentication of partner program execution and a communication device, and corresponds with the assembly of the public key of the signature check result by both program executions and the communication device The communication device with which both program executions and a communication device form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When one or more public keys showing the source origin of said program are obtained including the resource group for channels In case the process generated based on said program communicates, the communication device of both program executions and a communication device The program ID communication link range control approach according to claim 31 characterized by assigning a channel resource to one of the virtual channel resource groups corresponding to the public key showing the obtained source origin, and offering a channel using a virtual channel resource.

[Claim 33] The program ID communication link range control approach according to claim 27 or 32 characterized by the resource group for virtual channels being the socket defined virtually, and corresponding to each port of the socket which each of these virtual channel resource groups defined as this virtual target, and for the resource group for channels being the usual socket, and each of each channel resource groups corresponding to this socket each usual port.

[Claim 34] In the information system constituted by the program, and the program execution and the communication device which generate a process based on this program, and perform and communicate Said program execution and communication device include the process generated and performed based on said program. Said program The program body, The public key showing the source origin of this program, and the communication device which forms two or more virtual channels in per channel virtually, The resource for virtual channels whose one or more exist for every public key showing the source origin of said program, In case said program execution and communication device communicate by processing of the process generated based on said program including one or more resources for channels It is the channel offer approach the whole public key which makes a pair the resource for virtual channels required as the public key showing the source origin, and is characterized by including ***** which is made to correspond with a virtual channel and offers a channel using a virtual channel.

[Claim 35] It is the channel offer approach the whole public key according to claim 34 characterized by the resource group for virtual channels being the socket defined virtually, and corresponding to each port of the socket which each of these virtual channel resource groups defined as this virtual target, and for the resource group for channels being the usual socket, and each of each channel resource groups corresponding to this socket each usual port.

[Translation done.]

*** NOTICES ***

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the program authentication approach, the access-control approach of the processing generated by the communication link between programs in a distributed environment, and the communication link range control approach of the program in a distributed environment.

[0002]

[Description of the Prior Art] An example of the conventional information system For example, the program 1012 constituted by the program body 10121, and groups [showing the source origin of a program 1012 / the public key groups 101221-10122n and the private key groups 101241-10124n] pair as shown in drawing 19 , Are constituted by the process 10120 generated and performed by the pocket device 101 which are program execution and a communication device based on a program 1012. The principal part was constituted by the pocket device 101 which generates and performs a process 10120 for a program 1012 based on a program 1012, and the main phone machine 102 which are the communication link and processor which communicates with the pocket device 101.

[0003] As shown in drawing 19 , as for an example of the conventional information system, the principal part consisted of a program 1012, a pocket device 101 which are the program execution and the communication device which generates and performs a process 10120 based on a program 1012, and a main phone machine 102 which are the communication link and processor which communicates with the pocket device 101.

[0004] The program 112 was constituted including the program body 10121, the public key groups 101221-10122n showing the source origin of a program 1012, and the public key groups 101221-10122n and the private key groups 101241-10124n which make a pair.

[0005] The pocket device 101 consisted of the inclusion function part 1011, the process 10120 which performs a program 1012, a public key 10132 which accompanies the pocket device 101, a public key 10132 and the private key 10131 which makes a pair, and user password information 10190.

[0006] The main phone machine 102 was constituted including the public key 10132 which accompanies the pocket device 101 which is ID showing the partner who may communicate, and the user password information 10190 showing the user who may communicate.

[0007] Before the pocket device 101 communicates with the main phone machine 102 in such a conventional information system by processing of the process 10120 generated based on the program 1012 The process which obtains the public keys 101221-10122n showing the source origin of the program 1012 which the main phone machine 102 becomes from the pocket device 101 the origin of the process 10120 which makes the pocket device 101 communicate, The main phone machine 102 about each obtained public keys 101221-10122n By attesting by making the public key groups 101221-10122n and the private key groups 101241-10124n showing the source origin of the program 1012 which becomes the origin of the process 10120 which makes the pocket device 101 communicate used The program 1012 which becomes the origin of a process 10120 was also attesting suddenly all the public keys that succeeded in authentication.

[0008] Moreover, conventionally, as shown in drawing 20, as for other examples of an information system, the principal part consisted of a program 1012, a pocket device 101 which are the program execution and the communication device which generates and performs a process 10120 based on a program 1012, and a main phone machine 102 which are the communication link and processor which communicates with the pocket device 101.

[0009] The pocket device 101 consisted of the inclusion function part 1011, a process 10120 which performs a program 1012, the public key 10132 and private key 10131 which accompany the pocket device 101, and user password information 10190.

[0010] The main phone machine 102 has the public key 10132 which accompanies the pocket device 101 as a public key in which the partner who may communicate is shown, and the user password information 10190.

[0011] In such a conventional information system, by the pocket device 101, it attests about the user password information 10190, and the process 10120 which performs a program 1012 holds the user password information 10190. When a process 10120 tends to communicate with the main phone machine 102 and a communication link demand occurs, the main phone machine 102 From the pocket device 101, if it is reception, a public key 10132, and a match, a public key 10132 When it attests about a public key 10132 to the pocket device 101 and succeeds in authentication The access control about the processing which allows the communication link with the process 10120 and the main phone machine 102 which perform the program 1012 in the pocket device 101, and is generated by the communication link The user password information 10190 which is not based on a communications partner, but performs the same access control, or the process 10120 of a communications partner has was succeeded, and when user authentication was successful, the access control was performed based on it.

[0012] Furthermore, conventionally, as another example of an information system was shown in drawing 21, the principal part consisted of a pocket device 101 and a main phone machine 102.

[0013] The pocket device 101 was constituted including the inclusion function part 1011, a program 1012, the process 10120 that performs a program 1012, the private key 10131 which accompanies the pocket device 101, a private key 10131 and the public key 10132 which makes a pair, and the public key 10232 in which the partner who may communicate is shown.

[0014] The main phone machine 102 consisted of the inclusion function part 1021, a program 1022, the process 10220 that performs a program 1022, a private key 10231 which accompanies the main phone machine 102, a private key 10231 and the public key 10232 which accomplishes a pair, and a public key 10132 in which the partner who may communicate is shown.

[0015] With such a conventional information system, when a process 10120 and a process 10220 tend to communicate and a communication link demand occurs, the inclusion function parts 1011 and 1021 compare the public keys 10232 and 101032 in which the partner who may communicate public keys 10132 and 10232 with delivery and the received public keys 10232 and 10132 mutually is shown first, respectively. If each inclusion function parts 1011 and 1021 will perform mutual recognition with the received public keys 10232 and 10132 if in agreement, and mutual recognition is successful, the communication link with a process 10120 and a process 10220 will be allowed. When the public keys 10133 and 10233 in which the partner who may communicate with the received public keys 10232 and 10132 on the other hand is shown differed or the mutual recognition in public keys 10232 and 10132 went wrong, the communication link between a process 10120 and a process 10220 was not allowed. Moreover, the channel resource group was not virtually offered as another resource for every public key.

[0016]

[Problem(s) to be Solved by the Invention] In order to prevent ***** at the time of a communication link, as security level of the area (memory, disk, etc.) where a program exists, I hear that the 1st trouble cannot be read-out altered, and there is. The reason is that a program needs to have a private key.

[0017] The 2nd trouble is holding and carrying out the maintenance of the common information similar to user password information in a distributed environment. The reason is that it is necessary to share the information similar to the same user password information in order to attest.

[0018] The 3rd trouble is not being based on a communications partner but performing processing by the same authority wholly, when not using information similar to user password information. The reason is that it cannot acquire the information which can guarantee the justification for carrying out an access control.

[0019] At the time of a device, a program, or the design of a system, I hear that it must design according to an individual as which program the partner with whom a device, a program, or a process should communicate is considered, and there is the 4th trouble about it. the partner with whom a communications partner should communicate in the reason -- with, it is because it is decided by setup of the public key which must be.

[0020] I hear that the 5th trouble has much time and effort in the case of entrance of the escape of a system, and two or more systems, and it has it. The reason is that it must redesign separately as which program the partner with whom a device, a program, or a process should communicate at the time of the device for entrance of the escape of a system and two or more systems, a program, or the design of a system is considered.

[0021] The 6th trouble is that a system tends to become what was fixed to specific service. The reason is that there is much time and effort in the case of entrance of the escape of a system and two or more systems.

[0022] The 7th trouble is which channel being corresponded and used for which public key, and designing and managing. The reason is that it did not offer the channel resource group as another resource for every public key virtually.

[0023] The 1st purpose of this invention is to offer the private-key-less program authentication approach of preventing ***** in a communication link in the environment a read-out alteration being possible and good as security level of area where a program exists.

[0024] The 2nd purpose of this invention is to offer the program ID communications processing control approach for performing the access control of the processing generated by the communication link between programs in the distributed environment which is not in the bottom of a centralized control.

[0025] In a distributed environment, the range is beforehand limited about the range of communicative, i.e., informational circulation, and the 3rd purpose of this invention has a system design about the communication link range in offering the easy program ID communication link range control approach.

[0026] It is limited beforehand which channel is occupied by which object for public keys, and the 4th purpose of this invention has a system design about a channel in offering the channel offer approach the easy whole public key, when performing the communication link according to public key.

[0027] In addition, although there is JP,2000-148469,A as advanced-technology reference, the "access control to service between modular applications" approach indicated by this official report provides the 1st computer program module with access to service, when the 1st computer program module judges whether the power which gives access of service was signed in digital one and signed in digital one in it from the 2nd computer program module. However, this approach is for enabling it to perform the 1st computer program module and the 2nd computer program module in the same address space on the same computing node, and is not for making it make a different program on different program execution and communication device like this invention collaborate through a communication link so that the 1st computer program module can access service from the 2nd computer program module.

[0028]

[Means for Solving the Problem] The program execution and the communication device which the private-key-less program authentication approach of this invention generates a process based on a program and this program, and is performed, In the information system constituted by the communication link and processor which communicates with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key showing the source origin of this program and the signature performed to

said program body with this public key and the private key which makes a pair are included. The process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When it is able to be checked that said signature is generated with the public key showing the source origin of said program body and said program and the private key which makes a pair The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained, it is characterized by including the process which said communication link and processor attest with expressing the source origin of said program for this public key.

[0029] Moreover, the private-key-less program authentication approach of this invention In the process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair Said signature consists of a signature value enciphered with the public key which expresses the source origin of said program for the digest which carried out hashing of said program body by the Hash Function, and the private key which makes a pair. While said program execution and communication device decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program body by the Hash Function, and a digest is obtained. It is characterized by judging whether both digests are in agreement.

[0030] Furthermore, the private-key-less program authentication approach of this invention In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device It judges whether the public key in which said communication link and processor equip with the public key in which the partner who may communicate is shown, and the partner who may this communicate is shown, and the public key which accompanies said program execution and communication device are in agreement, and when in agreement, it is characterized by attesting said program execution and communication device.

[0031] Further again the private-key-less program authentication approach of this invention In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication device.

[0032] Moreover, the private-key-less program authentication approach of this invention In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The

public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key group showing the source origin of this program and the signature group performed with each public key and each private key which makes a pair to the data created combining said program body and said public key group are included. It checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair. The process which obtains the assembly of the public key corresponding to the signature by which being generated was checked, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained Said communication link and processor are characterized by including the process which attests each public key of the signature check result by said program execution and communication device with expressing the source origin of said program.

[0033] Furthermore, the private-key-less program authentication approach of this invention It checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair. In the process which obtains the assembly of the public key corresponding to the checked signature Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created in the combination of said program body and said public key group by the Hash Function, and each private key which makes a pair. Said program execution and communication device Carry out hashing of the data created in the combination of said program body and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by the Hash Function, and a digest is obtained. It is characterized by judging whether this digest and said digest group are in agreement.

[0034] Further again the private-key-less program authentication approach of this invention In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device It judges whether the public key in which said communication link and processor equip with the public key in which the partner who may communicate is shown, and the partner who may this communicate is shown, and the public key which accompanies said program execution and communication device are in agreement, and when in agreement, it is characterized by attesting said program execution and communication device.

[0035] Moreover, the private-key-less program authentication approach of this invention In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which

accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication device.

[0036] On the other hand, the method of program ID communications processing control of this invention In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device Said program contains the program body and ID group showing the source origin of this program. Said program execution and communication device include the process generated and performed based on said program. Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program When the process which obtains a part or all of ID group to which said communication link and processor express the source origin of the program which becomes the origin of said process, and one or more ID showing said source origin are obtained In the process at which said communication link and processor communicate with said program execution and communication device by processing of the process generated based on said program, and the processing generated by communication link It is characterized by including the process which performs the access control carried out based on ID group to which said communication link and processor express said source origin obtained from said program execution and management equipment.

[0037] Moreover, the program ID communications processing control approach of this invention In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device Said program contains the program body, the public key showing the source origin of this program, and this public key and the private key which makes a pair. Said program execution and communication device include the process generated and performed based on said program. Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process which obtains the public key showing the source origin of said program which said communication link and processor become from said program execution and communication device the origin of the process which makes this program execution and communication device communicate, When said program is attested with the process which attests said program with the public key system using the public key and private key with which said communication link and processor express the source origin of said program Said communication link and processor are characterized by including the process which communicates with said program execution and communication device by the access control carried out based on said public key.

[0038] Furthermore, the program ID communications processing control approach of this invention In the process which attests said program with the public key system using the public key and private key with which said communication link and processor express the source origin of said program about the obtained public key The one-time password method by the public key is used. Said program execution and communication device Delivery, and said communication link and processor a character string random to said program execution and communication device to said communication link and processor for said public key Delivery, The character string as which said program execution and communication device enciphered this character string with said private key is returned to said communication link and processor. If the character string which said communication link and processor decoded the enciphered character string with said sent public key, and decoded, and the character string sent previously are in agreement, it will be characterized by attesting said program.

[0039] Further again the program ID communications processing control approach of this

invention In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key showing the source origin of this program and the signature performed to said program body with this public key and the private key which makes a pair are included. The process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When it is able to be checked that said signature is generated with the public key showing the source origin of said program body and said program and the private key which makes a pair The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained Said communication link and processor obtain the public key showing the source origin of said program from said program execution and communication device, and is characterized by including the process which communicates with said program execution and communication device by the access control carried out based on this public key.

[0040] Moreover, the program ID communications processing control approach of this invention In the process which checks whether said program execution and communication device are generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair Said signature consists of a signature value enciphered with the public key which expresses the source origin of said program for the digest which carried out hashing of said program body by the Hash Function, and the private key which makes a pair. While said program execution and communication device decode said signature value with the public key showing the source origin of said program and obtaining a digest, carry out hashing of said program body by the Hash Function, and a digest is obtained. It is characterized by judging whether both digests are in agreement.

[0041] Furthermore, it is characterized by to judge whether the public key with which said communication link and processor is equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication device in the process with which said communication link and processor attests said program execution and communication device with the public key system using the public key and the private key which accompanies said program execution and communication device, and the public key of the program ID communications-processing control approach of this invention in which said partner who may communicate is shown correspond.

[0042] Further again the program ID communications processing control approach of this invention In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor If it decodes with the

public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication device.

[0043] Moreover, the program ID communications processing control approach of this invention In the information system constituted by the program, the program execution and the communication device which generate and perform a process based on this program, and the communication link and processor which communicate with this program execution and communication device The public key and private key with which said program execution and communication device accompany this program execution and communication device, The process generated and performed based on said program is included. Said program The program body, The public key group showing the source origin of this program and the signature group performed with each public key and each private key which makes a pair to the data created combining said program body and said public key group are included. It checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair. The process which obtains the assembly of the public key corresponding to the signature by which being generated was checked, Before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program The process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device, When one or more public keys corresponding to the signature by which said thing [being generated] was checked are obtained The process which obtains the public key with which said communication link and processor express the source origin of said program before said program execution and communication device communicate with said communication link and processor by processing of the process generated based on said program, When the public key which succeeds in authentication of said program execution and communication device, and expresses the source origin of said program is able to be obtained Said communication link and processor are characterized by including the process which communicates with said program execution and communication device by the access control carried out based on a part or all of an assembly of a public key by said program execution and communication device. [of a signature check result]

[0044] Furthermore, the program ID communications processing control approach of this invention In the process which checks whether said program execution and communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program body and said public key group by the Hash Function, and each private key which makes a pair. Said program execution and communication device It is characterized by judging whether each digest which decoded each signature value with each public key, respectively, and the digest obtained by carrying out hashing of the data created combining said program body and said public key group by the Hash Function are in agreement.

[0045] It is characterized by to judge whether the public key with which said communication link and processor is equipped with the public key in which the partner who may communicate is shown, and accompanies said program execution and communication device in the process with which said communication link and processor attests said program execution and communication device with the public key system using the public key and the private key which accompanies said program execution and communication device, and the public key of the program ID communications-processing control approach of this invention in which said partner who may communicate is shown correspond further again.

[0046] Moreover, the program ID communications processing control approach of this invention In the process with which said communication link and processor attest said program execution and communication device with the public key system using the public key and private key which accompany said program execution and communication device The one-time password method by the public key is used. Said communication link and processor A random character string to said program execution and communication device delivery, and said program execution and communication device This character string is enciphered with the private key which accompanies this program execution and communication device, and it returns to said communication link and processor. Said communication link and processor If it decodes with the public key in which the partner who holds the enciphered character string in advance, and who may communicate is shown and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting said program execution and communication device.

[0047] On the other hand, the program ID communication link range control approach of this invention In the information system constituted by the program, and two or more program executions and communication devices which generate a process, respectively and perform it based on these programs Said program contains the program body and ID group showing the source origin of this program. A certain process which the program execution and the communication device which exists based on a certain program generated Before communicating with a certain another process to which another a certain program execution and communication device generated this program or a certain another program to origin When ID group which expresses said source origin as the process which obtains a part or all of ID group to which both program executions and a communication device express the source origin of said program which becomes the origin of the process in partner program execution and a communication device is obtained ID group showing the source origin of said program which becomes ID group to which both program executions and a communication device express the obtained source origin, and the origin of the process in self-program execution and a communication device is compared. If one or more ID showing the source origin of said program in agreement exists, it will be characterized by including the process which opens a channel.

[0048] Moreover, the program ID communication link range control approach of this invention In the information system constituted by the program, and two or more program executions and communication devices which generate and perform each process based on each program Said program contains the program body, the public key showing the source origin of this program, and this public key and the private key which makes a pair. A certain process which the program execution and the communication device which exists based on a certain program generated Before communicating with a certain another process to which another a certain program execution and communication device generated this program or a certain another program to origin The process which obtains the public key with which both program executions and a communication device express the source origin of said program which consists of partner program execution and a communication device the origin of the process in partner program execution and a communication device, respectively, The process which judges whether the public key showing the source origin of said program which both program executions and a communication device become the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement, The process which performs mutual recognition of the program which both program executions and a communication device become the origin of the process in partner program execution and a communication device using the public key and private key showing the source origin of said program which becomes the origin of the process in partner program execution and a communication device, The public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement. And when mutual recognition of the program which becomes the origin of the process in partner program execution and a communication device is carried out, both program executions and a communication device are characterized by including

the process which opens a channel.

[0049] Moreover, the program ID communication link range control approach of this invention In the process which performs mutual recognition of the program which both program executions and a communication device become the origin of the process in partner program execution and a communication device using the public key and private key showing the source origin of said program which becomes the origin of the process in partner program execution and a communication device The one-time password method by the public key is used. Both program executions and a communication device The public key which accompanies self-program execution and a communication device to partner program execution and a communication device Delivery, A random character string to partner program execution and a communication device, respectively Delivery, The character string enciphered with the public key with which partner program execution and a communication device express the source origin of said program which becomes the origin of the process in partner program execution and a communication device about this character string, and the private key which makes a pair is returned to self-program execution and a communication device. If self-program execution and a communication device decode the enciphered character string with a corresponding public key and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting the program which becomes the origin of the process in partner program execution and a communication device communication device.

[0050] Furthermore, the program ID communication link range control approach of this invention In the information system constituted by the program, and two or more program executions and communication devices which generate and perform each process based on each program The public key and private key with which said program execution and communication device accompany self-program execution and a communication device, The public key which accompanies partner program execution and a communication device, and the process generated and performed based on said program are included. Said program The program body, The public key showing the source origin of this program and the signature performed to said program body with this public key and the private key which makes a pair are included. A certain process which the program execution and the communication device which exists based on a certain program generated Before communicating with a certain another process to which another a certain program execution and communication device generated this program or a certain another program to origin The process which checks whether both program executions and a communication device are generated by the public key with which said signature expresses the source origin of said program body and said said program, and the private key which makes a pair, The process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device before performing said communication link, When it is able to be checked that both program executions and a communication device are generated with the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair The process which transmits said public key to partner program execution and a communication device before performing said communication link, The process which judges whether the public key showing the source origin of said program which both program executions and a communication device become the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement, Mutual recognition of the program which becomes the origin of the process in partner program execution and a communication device is carried out. And when the public key showing the source origin of said program which becomes the origin of the process in the public key obtained from partner program execution and a communication device, and self-program execution and a communication device is in agreement, both program executions and a communication device are characterized by including the process which opens a channel.

[0051] Further again the program ID communication link range control approach of this invention In the process which checks whether both program executions and a communication device are

generated by the public key with which said signature expresses the source origin of said program body and said program, and the private key which makes a pair. Said signature consists of a signature value enciphered with the public key which expresses the source origin of said program for the digest which carried out hashing of said program body by the Hash Function, and the private key which makes a pair. While both program executions and a communication device decode said signature value with the public key showing the source origin of said program and obtaining a digest, hashing of said program body is carried out by the Hash Function, and a digest is obtained and it is characterized by judging whether both digests are in agreement.

[0052] Moreover, the program ID communication link range control approach of this invention In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device It is characterized by judging whether the public key in which both program executions and a communication device equip with the public key in which the partner who may communicate is shown, and the partner who may this communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication device are in agreement.

[0053] Furthermore, the program ID communication link range control approach of this invention In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device The one-time password method by the public key is used. Self-program execution and a communication device The public key which accompanies partner program execution and a communication device is obtained from partner program execution and a communication device. A random character string to partner program execution and a communication device delivery, and partner program execution and a communication device This character string is enciphered with the private key which accompanies partner program execution and a communication device, and it returns to self-program execution and a communication device. Self-program execution and a communication device If it decodes with said public key which obtained the enciphered character string from partner program execution and a communication device and the decoded character string and the character string sent previously are in agreement, it will be characterized by attesting partner program execution and a communication device.

[0054] Further again the program ID communication link range control approach of this invention When there is a public key both program executions and a communication device succeed in authentication of partner program execution and a communication device, and corresponds with the assembly of the public key of the signature check result by both program executions and the communication device The communication device with which both program executions and a communication device form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When the public key showing the source origin of said program is obtained including the resource group for channels In case the process generated based on said program communicates, a channel resource is assigned to one of the virtual channel resource groups corresponding to the public key with which the communication device of both program executions and a communication device expresses the obtained source origin, and it is characterized by offering a channel using a virtual channel resource.

[0055] Moreover, the program ID communication link range control approach of this invention In the information system constituted by the program, and two or more program executions and communication devices which generate and perform each process based on each program The public key and private key with which said program execution and communication device accompany self-program execution and a communication device, The public key which accompanies partner program execution and a communication device, and the process generated and performed based on each program are included. Each program The program body, The public key group showing the source origin of this program and the signature group performed with

each public key and each private key which makes a pair to the data created combining said program body and said public key group are included. The process which checks whether both program executions and a communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair, and both program executions and a communication device. The process which attests partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device, Both program executions and a communication device tell the assembly of the public key of the signature check result by self-program execution and the communication device to partner program execution and a communication device. The process which judges whether there is any public key which is in agreement with the assembly of the public key of the signature check result by self-program execution and the communication device and the assembly of the public key of the signature check result by partner program execution and the communication device, One or more public keys which succeed in authentication of partner program execution and a communication device, and are in agreement with the assembly of the public key of the signature check result by both program executions and the communication device are characterized by both program executions and a communication device including the process which opens the channel between processes at a certain time.

[0056] Furthermore, the program ID communication link range control approach of this invention In the process which judges whether both program executions and a communication device are generated by the data with which each signature was created combining said program body and said public key group, each public key corresponding to each signature, and each private key which makes a pair Each signature consists of each signature value enciphered with each public key which expresses the source origin of said program for the digest which carried out hashing of the data created combining said program body and said public key group by the Hash Function, and each private key which makes a pair. Partner program execution and a communication device Carry out hashing of the data created by said program body and said public key group while decoding each signature value with each public key showing the source origin of said program, respectively and obtaining the digest group by the Hash Function, and a digest is obtained. It is characterized by judging whether this digest and said digest group are in agreement.

[0057] Further again the program ID communication link range control approach of this invention In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device It is characterized by judging whether the public key in which both program executions and a communication device equip with the public key in which the partner who may communicate is shown, and the partner who may this communicate is shown, and one or more public keys of the public key group which accompanies partner program execution and a communication device are in agreement.

[0058] Moreover, the program ID communication link range control approach of this invention In the process with which both program executions and a communication device attest partner program execution and a communication device with the public key system using the public key and private key which accompany partner program execution and a communication device The one-time password method by the public key is used. Self-program execution and a communication device The public key which accompanies partner program execution and a communication device is obtained from partner program execution and a communication device. A random character string to partner program execution and a communication device delivery, and partner program execution and a communication device This character string is enciphered with the private key which accompanies partner program execution and a communication device, and it returns to self-program execution and a communication device. Self-program execution and a communication device If it decodes with said public key which obtained the enciphered character string from partner program execution and a communication device and the decoded

character string and the character string sent previously are in agreement, it will be characterized by attesting partner program execution and a communication device.

[0059] Furthermore, the program ID communication link range control approach of this invention When there is a public key both program executions and a communication device succeed in authentication of partner program execution and a communication device, and corresponds with the assembly of the public key of the signature check result by both program executions and the communication device The communication device with which both program executions and a communication device form two or more virtual channels in per channel virtually in the process which opens the channel between processes, The resource group for virtual channels showing the source origin of said program which exists for every public key, When one or more public keys showing the source origin of said program are obtained including the resource group for channels In case the process generated based on said program communicates, a channel resource is assigned to one of the virtual channel resource groups corresponding to the public key with which the communication device of both program executions and a communication device expresses the obtained source origin, and it is characterized by offering a channel using a virtual channel resource.

[0060] The resource group for virtual channels is the socket defined virtually, it corresponds to each port of the socket which each of these virtual channel resource groups defined as this virtual target, the resource group for channels is the usual socket, and the program ID communication link range control approach of this invention is characterized by each of each channel resource groups corresponding to this socket each usual port further again.

[0061] In the information system constituted on the other hand by the program execution and the communication device which the channel offer approach generates a process based on a program and this program, and performs and communicates the whole public key of this invention Said program execution and communication device include the process generated and performed based on said program. Said program The program body, The public key showing the source origin of this program, and the communication device which forms two or more virtual channels in per channel virtually, The resource for virtual channels whose one or more exist for every public key showing the source origin of said program, In case said program execution and communication device communicate by processing of the process generated based on said program including one or more resources for channels The resource for virtual channels required as the public key showing the source origin is made into a pair, and it is made to correspond with a virtual channel and is characterized by including ***** which offers a channel using a virtual channel.

[0062] The whole public key of this invention, the resource group for virtual channels is the socket defined virtually, it corresponds to each port of the socket which each of these virtual channel resource groups defined as this virtual target, the resource group for channels is the usual socket, and the channel offer approach is characterized by each of each channel resource groups corresponding to this socket each usual port further again.

[0063]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail with reference to a drawing.

[0064] (1) The principal part consists of programs 112 which the information system with which the private-key-less program authentication approach concerning the gestalt of operation of the 1st of this invention was applied when gestalt drawing 1 of the 1st operation was referred to is installed in the pocket device 11 by which the program execution and the communication device which has an execution function and communication facility was applied, the main phone machine 12 with which the communication link and the processor which has communication facility was applied, and the pocket device 11, and are performed.

[0065] As for an execution function and communication facility, Java (trademark of Sun Microsystems, Inc.) etc. is assumed.

[0066] As a pocket device 11, a portable telephone (PHS (Personal HandyPhone) is included), a Personal Digital Assistant, etc. are assumed.

[0067] A POS (Point Of Sales) terminal etc. is assumed as a main phone machine 12.

[0068] Communication facility between the pocket device 11 and the main phone machine 12 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN (Local Area Network), and PIAFS (PHS Internet Access Forum Standard).

[0069] The pocket device 11 is constituted including the reliable inclusion function part 111, the process 1120 which performs a program 112, and the private key 1131 and public key 1132 which accompany the pocket device 11.

[0070] The program 112 is constituted including the hash value 11231 which is the signature (a digital signature, electronic signature) which enciphered the public key 11221 and the pair with the private key (not shown) to make in the program body 1121, the public key 11221 showing the source origin of a program 112, and the digest that carried out hashing of the program body 1121 by the Hash Function. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 112, the program body 1121, the public key 11221, and the hash value 11231 are created as one.

[0071] The main phone machine 12 has the public key 1132 which accompanies the pocket device 11 as a public key in which the partner who may communicate is shown.

[0072] If drawing 2 is referred to, processing of the inclusion function part 111 of the pocket device 11 and the main phone machine 12 will consist of the hash value check step S101, the communication link demand generating step S102, the pocket device authentication step S103, the program source origin judging step S104, a program authentication step S105, and program a non-attested step S106.

[0073] Next, actuation of the information system with which the private-key-less program authentication approach concerning the gestalt of the 1st operation constituted in this way was applied is explained to a detail with reference to drawing 1 and drawing 2.

[0074] First, the pocket device 11 checks whether a hash value 11231 is generated by the program body 1121 and a public key 11221, and the private key that makes a pair by the inclusion function part 111 (step S101). While obtaining the digest which the inclusion function part 111 decoded the hash value 11231 with the public key 11221, and carried out hashing of the program body 1121 in detail, it is verifying whether hashing of the program body 1121 being carried out by the known Hash Function, a digest's being obtained, and both digests being completely in agreement, and a hash value 11231 checks whether it is generated by the program body 1121 and a public key 11221, and the private key that makes a pair. That is, the program body 1121 and a public key 11221 were not altered, and it checks that a program 112 has the Shinsei source origin. In addition, this check processing should just be performed once, when a program 112 introduced for example, downloads to the pocket device 11.

[0075] Next, when the process 1120 which performs the program 112 in the pocket device 11 tends to communicate with the main phone machine 12 and a communication link demand is generated (step S102), the main phone machine 12 attests the pocket device 11 before it with the public key system using the public key 1132 and private key 1131 which accompany the pocket device 11 (step S103).

[0076] For example, it judges whether the public key 1132 which accompanies the pocket device 11 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 1132 of the main phone machine 12 which accompanies the pocket device 11 which the pocket device 11 holds correspond, and when in agreement, the pocket device 11 is attested.

[0077] Moreover, when the one-time password (One Time Password) method by the public key of RSA (Rivest, Shamir, Adleman) is used, The main phone machine 12 a random character string to the pocket device 11 Delivery ("Challenge"). The inclusion function part 111 of the pocket device 11 enciphers the character string with the private key 1131 which accompanies the pocket device 11, and returns it to the main phone machine 12 ("Response"). If the main phone machine 12 is decoded with the public key 1132 which accompanies the pocket device 11 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The pocket device 11 is attested with his being the partner (that is,

thing which owns the public key 1232 which accompanies the pocket device 11 held as a public key in which the partner who may communicate is shown, and the private key 1131 which makes a pair) who may communicate.

[0078] When it succeeds in authentication of the pocket device 11, the main phone machine 12 obtains the public key 11221 of the hash value check result by the pocket device 11 from the inclusion function part 111 of the pocket device 11, judges whether it is that in which a program 112 has the Shinsei source origin based on the hash value check result by the pocket device 11 (step S104), and presupposes that the program 112 was attested with the public key 11221 obtained when that was right (step S105).

[0079] On the other hand, when authentication of the pocket device 11 goes wrong (step S103), or when it is not the public key with which a public key 11221 expresses the Shinsei source origin of a program 112 (step S104), the main phone machine 12 does not attest a program 112.

[0080] Even if a program 112 does not have a private key, according to the gestalt of the 1st operation, the main phone machine 12 From authentication of the program 112 which becomes the origin of the process 1120 in the pocket device 11 which is going to communicate with the main phone machine 12 being possible When communicating with the pocket device 11 which carries out based on the program 112 which steals and is under the environment in which a **** alteration is possible, and operates, the main phone machine 12 can prevent ***** of a program 112, and it can attest.

[0081] (2) The principal part consists of programs 212 which the information system with which the private-key-less program authentication approach concerning the gestalt of operation of the 2nd of this invention was applied when gestalt drawing 3 of the 2nd operation was referred to is installed in the pocket device 21 by which the program execution and the communication device which has an execution function and communication facility was applied, the main phone machine 22 with which the communication link and the processor which has communication facility was applied, and the pocket device 21, and are performed.

[0082] As for an execution function and communication facility, Java etc. is assumed.

[0083] As a pocket device 21, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0084] A POS terminal etc. is assumed as a main phone machine 22.

[0085] Communication facility between the pocket device 21 and the main phone machine 22 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0086] The pocket device 21 is constituted including the reliable inclusion function part 211, the process 2120 which performs a program 212, and the private key 2131 and public key 2132 which accompany the pocket device 21.

[0087] Programs 212 are the public key groups 21221-2122n (n is two or more positive integers.) which express the source origin of a program 212 as the program body 2121. The digest which carried out hashing of the data created combining the program body 2121 and the public key groups 21221-2122n by the Hash Function is constituted including that it is the same as that of the following, and the hash value groups 21231-2123n which are signature groups which enciphered each public keys 21221-2122n and a pair with each private key (not shown) to make, respectively. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 212, the program body 2121, the public key groups 21221-2122n, and the hash value groups 21231-2123n are created as one.

[0088] The main phone machine 22 has the public key 2132 which accompanies the pocket device 21 as a public key in which the partner who may communicate is shown.

[0089] If drawing 4 is referred to, processing of the inclusion function part 211 of the pocket device 21 and the main phone machine 22 will consist of the hash value check step S201, the communication link demand generating step S202, the pocket device authentication step S203, the program origin judging step S204, a program authentication step S205, and program a non-attested step S206.

[0090] Next, actuation of the information system with which the private-key-less program authentication approach concerning the gestalt of the 2nd operation constituted in this way was

applied is explained to a detail with reference to drawing 3 and drawing 4.

[0091] First, the pocket device 21 obtains the assembly of the public key corresponding to the hash value which each hash values 21231-2123n checked whether it would be generated by the program body 2121 and the public key groups 21221-2122n, each public keys 21221-2122n, and each private key that makes a pair, and checked by the inclusion function part 211 (step S201). In detail the inclusion function part 211 While obtaining the digest group which carried out hashing of the data which decoded each hash values 21231-2123n with each public keys 21221-2122n, respectively, and were created combining the program body 2221 and the public key groups 21221-2122n Carry out hashing of the data created combining the program body 2121 and the public key groups 21221-2122n by the known Hash Function, and a digest is obtained. By verifying, respectively, whether this digest and each of digest groups are completely in agreement It checks, respectively whether each hash values 21231-2123n are generated by the program body 2121 and the public key groups 21221-2122n, each public keys 21221-2122n, and each private key that makes a pair. The assembly of the public key corresponding to the checked hash value is obtained. That is, the program body 2121 and the public key groups 21221-2122n were not altered, and check that a program 212 has the Shinsei source origin. In addition, this check processing should just be performed once, when a program 212 introduced for example, downloads to the pocket device 21.

[0092] Next, when the process 2120 which performs the program 212 in the pocket device 21 tends to communicate with the main phone machine 22 and a communication link demand occurs (step S202), the main phone machine 22 attests the pocket device 21 before it with the public key system using the private key 2131 and public key 2132 which accompany the pocket device 21 (step S203).

[0093] For example, it judges whether the public key 2132 which accompanies the pocket device 21 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 2132 of the main phone machine 22 which accompanies the pocket device 21 which the pocket device 21 holds correspond, and when in agreement, the pocket device 21 is attested.

[0094] Moreover, when the one-time password method by the public key of RSA is used, The main phone machine 22 a random character string to the pocket device 21 Delivery ("Challenge"), The inclusion function part 211 of the pocket device 21 enciphers the character string with the private key 2131 which accompanies the pocket device 21, and returns it to the main phone machine 22 ("Response"). If the main phone machine 22 is decoded with the public key 2132 which accompanies the pocket device 21 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The pocket device 21 is attested with his being the partner (that is, thing which owns the public key 2132 which accompanies the pocket device 21 held as a public key in which the partner who may communicate is shown, and the private key 2131 which makes a pair) who may communicate.

[0095] When it succeeds in authentication of the pocket device 21, the main phone machine 22 The assembly of the public key of the hash value check result by the pocket device 21 is obtained from the inclusion function part 211 of the pocket device 21. It judges with it being that in which a program 212 has the Shinsei source origin if one or more public keys are contained in the assembly of the public key of the hash value check result by the pocket device 21 (step S204). Suppose that the program 212 was attested by a part or all of an assembly of a public key (step S205).

[0096] On the other hand, when authentication of the pocket device 21 goes wrong (step S203), or when the public key showing the Shinsei source origin of a program 212 is not obtained (step S204), the main phone machine 22 does not attest a program 212 (step S206).

[0097] In addition, although it judged with it being that in which a program 212 has the Shinsei source origin with the gestalt of implementation of the above 2nd when one or more public keys were contained in the assembly of the public key of the hash value check result by the pocket device 21 at step S204 Only when public key groups [21221-2122n] all are contained in the assembly of the public key of the hash value check result by the pocket device 21, it can judge

with it being that in which a program 212 has the Shinsei source origin.

[0098] Since the hash value groups 21231-2123n which are signature groups are given to the public key groups 21221-2122n held with the program body 2121 when allowing a program 212 to have the public key groups 21221-2122n according to the gestalt of the 2nd operation, ***** of a program can be prevented.

[0099] (2) The principal part consists of programs 312 which the information system with which the program ID communications-processing control approach concerning the gestalt of operation of the 3rd of this invention was applied when gestalt drawing 5 of the 3rd operation was referred to is installed in the pocket device 31 by which the program execution and the communication device which has an execution function and communication facility was applied, the main phone machine 32 with which the communication link and the processor which has communication facility was applied, and the pocket device 31, and are performed.

[0100] As for an execution function and communication facility, Java etc. is assumed.

[0101] As a pocket device 31, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0102] A POS terminal etc. is assumed as a main phone machine 32.

[0103] Communication facility between the pocket device 31 and the main phone machine 32 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0104] The pocket device 31 is constituted including the reliable inclusion function part 311 and the process 3120 which performs a program 312.

[0105] The program 312 is constituted including the program body 3121, and the public key 31221 and private key 31241 showing the source origin of a program 312. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 312, the program body 3121, the public key 31221, and the private key 31241 are created as one.

[0106] If drawing 6 is referred to, processing of the inclusion function part 311 of the pocket device 31 and the main phone machine 32 will consist of the communication link demand generating step S301, the public key acquisition step S302, the program authentication step S303, a communication link / processing step S304, and a processing[a communication link /]-less step S305.

[0107] Next, actuation of the information system with which the program ID communications processing control approach concerning the gestalt of the 3rd operation constituted in this way was applied is explained to a detail with reference to drawing 5 and drawing 6.

[0108] When a communication link demand for the process 3120 which performs the program 312 in the pocket device 31 to communicate with the main phone machine 32 is generated (step S301), the main phone machine 32 obtains the public key 31221 showing the source origin of the program 312 which becomes the origin of a process 3120 through the inclusion function part 311 of the pocket device 31 (step S302).

[0109] Next, it attests whether the main phone machine 32 is that in which the program 312 which becomes the origin of a process 3120 with the public key system using a public key 31221 and a private key 31241 has the Shinsei source origin to the inclusion function part 311 of the pocket device 31 (step S303).

[0110] For example, when the one-time password method by the public key of RSA is used, The main phone machine 32 a random character string in the inclusion section 311 of the pocket device 31 Delivery ("Challenge"), Encipher with the public key 31221 showing the source origin of the program 312 which becomes the origin of a process 3120 about the character string, and the private key 31241 which makes a pair, and the inclusion function part 311 of the pocket device 31 is returned to the main phone machine 32 ("Response"). If the main phone machine 32 is decoded with the public key 31221 which received the enciphered character string previously and the decoded character string and the random character string sent previously are in agreement It attests with the program 312 which becomes the origin of a process 3120 being a thing with the Shinsei source origin (that is, a program 312 owning the public key 31221 showing the source origin of this program 312, and the private key 31241 which makes a pair).

[0111] When it succeeds in authentication of a program 312 (step S303), the main phone

machine 32 carries out the access control of the processing generated by subsequent communication links by the user authority corresponding to a public key 31221, and is performed (step S304).

[0112] On the other hand, when authentication of a program 312 goes wrong (step S303), or when the user authority corresponding to a public key 31221 does not exist, the main phone machine 32 performs processing by the user authority to have not carried out processing generated by communication link, or for specification to have been restricted (step S305).

[0113] According to the gestalt of the 3rd operation, since it communicates with the public key 31221 showing the source origin of a program 312, i.e., the access control carried out based on the information similar to the manufacturer and the version of a program 312, security can be maintained to a malicious program.

[0114] Moreover, since it communicates with the public key 31221 showing the source origin of a program 312, i.e., the access control carried out based on the information similar to the manufacturer and the version of a program 312, a centralized control like user management can maintain security to a malicious program about processing by the communication link under a difficult distributed environment.

[0115] (4) The principal part consists of programs 412 which the information system with which the program ID communications-processing control approach concerning the gestalt of operation of the 4th of this invention was applied when gestalt drawing 7 of the 4th operation was referred to is installed in the pocket device 41 by which the program execution and the communication device which has an execution function and communication facility was applied, the main phone machine 42 with which the communication link and the processor which has communication facility was applied, and the pocket device 41, and are performed.

[0116] As for an execution function and communication facility, Java etc. is assumed.

[0117] As a pocket device 41, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0118] A POS terminal etc. is assumed as a main phone machine 42.

[0119] Communication facility between the pocket device 41 and the main phone machine 42 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0120] The pocket device 41 is constituted including the reliable inclusion function part 411, the process 4120 which performs a program 412, and the private key 4131 and public key 4132 which accompany the pocket device 41.

[0121] The program 412 is constituted including the hash value 41231 which is the signature which enciphered the public key 41221 and the pair with the private key (not shown) to make in the program body 4121, the public key 41221 showing the source origin of a program 412, and the digest that carried out hashing of the program body 4121 by the Hash Function. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 412, the program body 4121, the public key 41221, and the hash value 41231 are created as one.

[0122] The main phone machine 42 has the public key 4132 which accompanies the pocket device 41 as a public key in which the partner who may communicate is shown.

[0123] If drawing 8 is referred to, processing of the inclusion function part 411 of the pocket device 41 and the main phone machine 42 will consist of the hash value check step S401, the communication link demand generating step S402, the pocket device authentication step S403, the program source origin judging step S404, a communication link / processing step S405, and a processing[a communication link /]-less step S406.
 [0124] Next, actuation of the information system with which the program ID communications processing control approach concerning the gestalt of the 4th operation constituted in this way was applied is explained to a detail with reference to drawing 7 and drawing 8.

[0125] First, the pocket device 41 checks whether a hash value 41231 is generated by the program body 4121 and a public key 41221, and the private key that makes a pair by the inclusion function part 411 (step S401). While obtaining the digest which the inclusion function part 411 decoded the hash value 41231 with the public key 41221, and carried out hashing of the program body 4121 in detail, it is verifying whether hashing of the program body 4121 being

carried out by the known Hash Function, a digest's being obtained, and both digests being completely in agreement, and a hash value 41231 checks whether it is generated by the program body 4121 and a public key 41221, and the private key that makes a pair. That is, the program body 4121 and a public key 41221 were not altered, and it checks that a program 412 has the Shinsei source origin. In addition, this check processing should just be performed once, when a program 412 introduced for example, downloads to the pocket device 41.

[0126] Next, when the process 4120 which performs the program 412 in the pocket device 41 tends to communicate with the main phone machine 42 and a communication link demand is generated (step S402), the main phone machine 42 attests the pocket device 41 before it with the public key system using the public key 4132 and private key 4131 which accompany the pocket device 41 (step S403).

[0127] For example, it judges whether the public key 4132 which accompanies the pocket device 41 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 4132 of the main phone machine 42 which accompanies the pocket device 41 which the pocket device 41 holds correspond, and when in agreement, the pocket device 41 is attested.

[0128] Moreover, when the one-time password method by the public key of RSA is used, The main phone machine 42 a random character string to the pocket device 41 Delivery ("Challenge"), The inclusion function part 411 of the pocket device 41 enciphers the character string with the private key 4131 which accompanies the pocket device 41, and returns it to the main phone machine 42 ("Response"). If the main phone machine 42 is decoded with the public key 4132 which accompanies the pocket device 41 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The pocket device 41 is attested with his being the partner (that is, thing which owns the public key 4132 which accompanies the pocket device 41 held as a public key in which the partner who may communicate is shown, and the private key 4131 which makes a pair) who may communicate.

[0129] When it succeeds in authentication of the pocket device 41, the main phone machine 42 obtains a public key 41221 from the inclusion function part 411 of the pocket device 41, it judges whether it is that in which a program 412 has the Shinsei source origin based on the hash value check result by the pocket device 41 (step S404), and if that is right, it will carry out the access control of the processing generated by subsequent communication links by the user authority corresponding to a public key 41221, and will perform it (step S405).

[0130] When it is not that in which a program 412 has the Shinsei source origin on the other hand when authentication of the pocket device 41 goes wrong (step S403) (step S404), or when the user authority corresponding to a public key 41221 does not exist, by the user authority to have not performed processing generated by communication link, or for specification to have been decided, the access control of the main phone machine 42 is carried out, and it is performed (step S406).

[0131] Even if a program 412 does not have a private key, according to the gestalt of the 4th operation, the main phone machine 42 From authentication of the program 412 which becomes the origin of the process 4120 in the pocket device 41 which is going to communicate with the main phone machine 42 being possible When communicating with the pocket device 41 which carries out based on the program 412 which steals and is under the environment in which a **** alteration is possible, and operates, the main phone machine 42 can prevent ***** of a program 412, and it can attest.

[0132] (5) The principal part consists of programs 512 which the information system with which the program ID communications-processing control approach concerning the gestalt of operation of the 5th of this invention was applied when gestalt drawing 9 of the 5th operation was referred to is installed in the pocket device 51 by which the program execution and the communication device which has an execution function and communication facility was applied, the main phone machine 52 with which the communication link and the processor which has communication facility was applied, and the pocket device 51, and are performed.

[0133] As for an execution function and communication facility, Java etc. is assumed.

[0134] As a pocket device 51, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0135] A POS terminal etc. is assumed as a main phone machine 52.

[0136] Communication facility between the pocket device 51 and the main phone machine 52 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0137] The pocket device 51 is constituted including the reliable inclusion function part 511, the process 5120 which performs a program 512, and the private key 5131 and public key 5132 which accompany the pocket device 51.

[0138] The program 512 is constituted including the hash value groups 51231-5123n which are signature groups which enciphered each public keys 51221-5122n and a pair with each private key (not shown) to make, respectively in the digest which carried out hashing of the data created combining the program body 5121, the public key groups 51221-5122n showing the source origin of a program 512, and the program body 5121 and the public key groups 51221-5122n by the Hash Function. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 512, the program body 5121, the public key groups 51221-5122n, and the hash value groups 51231-5123n are created as one.

[0139] The main phone machine 52 has the public key 5132 which accompanies the pocket device 51 as a public key in which the partner who may communicate is shown.

[0140] If drawing 10 is referred to, processing of the inclusion function part 511 of the pocket device 51 and the main phone machine 52 will consist of the hash value check step S501, the communication link demand generating step S502, the pocket device authentication step S503, the program source origin judging step S504, a communication link / processing step S505, and a processing[a communication link /]-less step S506.

[0141] Next, actuation of the information system with which the program ID communications processing control approach concerning the gestalt of the 5th operation constituted in this way was applied is explained to a detail with reference to drawing 9 and drawing 10.

[0142] First, the pocket device 51 obtains the assembly of the public key corresponding to the hash value which each hash values 51231-5123n checked whether it would be generated by the program body 5121 and the public key groups 51221-5122n, each public keys 51221-5122n, and each private key that makes a pair, and checked by the inclusion function part 511 (step S501). In detail the inclusion function part 511 While obtaining the digest group which carried out hashing of the data which decoded each hash values 51231-5123n with each public keys 51221-5122n, respectively, and were created combining the program body 5121 and the public key groups 51221-5122n Carry out hashing of the data created combining the program body 5121 and the public key groups 51221-5122n by the known Hash Function, and a digest is obtained. By verifying, respectively, whether this digest and each of digest groups are completely in agreement ** is checked [whether each hash values 51231-5123n are generated by the program body 5121 and the public key groups 51221-5122n, each public keys 51221-5122n, and each private key that makes a pair, and], respectively. The assembly of the public key corresponding to the checked hash value is obtained. That is, the program body 5121 and the public key groups 51221-5122n were not altered, and check that a program 512 has the Shinsei source origin. In addition, this check processing should just be performed once, when a program 512 introduced for example, downloads to the pocket device 51.

[0143] Next, when the process 5120 which performs the program 512 in the pocket device 51 tends to communicate with the main phone machine 52 and a communication link demand occurs (step S502), the main phone machine 52 attests the pocket device 51 before it with the public key system using the public key 5132 and private key 5131 which accompany the pocket device 51 (step S503).

[0144] For example, it judges whether the public key 5132 which accompanies the pocket device 51 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 5132 of the main phone machine 52 which accompanies the pocket device 51 which the pocket device 51 holds correspond, and when in agreement, the pocket device 51 is attested.

[0145] Moreover, when the one-time password method by the public key of RSA is used, The main phone machine 52 a random character string to the pocket device 51 Delivery ("Challenge"), The inclusion function part 511 of the pocket device 51 enciphers the character string with the private key 5131 which accompanies the pocket device 51, and returns it to the main phone machine 52 ("Response"). If the main phone machine 52 is decoded with the public key 5132 which accompanies the pocket device 51 held as a public key in which the partner who may communicate the enciphered character string in advance is shown and the decoded character string and the random character string sent previously are in agreement The pocket device 51 is attested with his being the partner (that is, thing which owns the public key 5132 which accompanies the pocket device 51 held as a public key in which the partner who may communicate is shown, and the private key 5131 which makes a pair) who may communicate.

[0146] When it succeeds in authentication of the pocket device 51, the main phone machine 52 The assembly of the public key of a hash value check result is obtained from the inclusion function part 511 of the pocket device 51. It judges with it being that in which a program 512 has the Shinsei source origin if one or more public keys are contained in the assembly of the public key of the hash value check result by the pocket device 51 (step S504). In the combination of the user authority corresponding to each public key of the assembly of the public key of a hash value check result, the access control of the processing generated by subsequent communication links is carried out, and it is performed (step S505).

[0147] When authentication of the pocket device 51 goes wrong (step S503) and it is not that in which a program 512 has the Shinsei source origin on the other hand (step S504), Or when one does not exist [the user authority corresponding to the public key in the assembly of the public key of the hash value check result by the pocket device 51], by the user authority to have not performed processing generated by communication link, or for specification to have been restricted, the access control of the main phone machine 52 is carried out, and it is performed (step S506).

[0148] In addition, although it judged with it being that in which a program 512 has the Shinsei source origin with the gestalt of implementation of the above 5th when one or more public keys were contained in the assembly of the public key of the hash value check result by the pocket device 51 at step S504 Only when public key groups [51221-5122n] all are contained in the assembly of the public key of the hash value check result by the pocket device 51, it can judge with it being that in which a program 512 has the Shinsei source origin.

[0149] According to the gestalt of the 5th operation From attaching the hash value groups 51231-5123n which are signature groups to the public key groups 51221-5122n held with the program body 5121, when allowing a program 512 to have the public key groups 51221-5122n showing the source origin of this program 512 ***** of a program 512 can be prevented, in the combination of the user authority corresponding to each public key of the assembly of the public key of a hash value check result, the access control of the processing generated by communication link can be carried out, and it can be performed.

[0150] (6) If gestalt drawing 11 of the 6th operation is referred to, the information system with which the program ID communication link range control approach concerning the gestalt of operation of the 6th of this invention was applied The pocket device 61 which has a program execution function and communication facility, and the main phone machine 62 which similarly has a program execution function and communication facility, The principal part consists of a program 612 which is installed in the pocket device 61 and performed, and a program 622 which is installed in the main phone machine 62 and performed.

[0151] As for an execution function and communication facility, Java etc. is assumed.

[0152] As a pocket device 61, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0153] A POS terminal etc. is assumed as a main phone machine 62.

[0154] The communication mode used for the communication facility between the pocket device 61 and the main phone machine 62 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0155] The pocket device 61 is constituted including the reliable inclusion function part 611 and

the process 6120 which performs a program 612.

[0156] The program 612 is constituted including the program body 6121, and the public key 6122 and private key 6124 showing the source origin of a program 612. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 612, the program body 6121, the public key 6122, and the private key 6124 are created as one.

[0157] The main phone machine 62 is constituted including the reliable inclusion function part 621 and the process 6220 which performs a program 622.

[0158] The program 622 is constituted including the program body 6221, and the public key 6222 and private key 6224 showing the source origin of a program 622. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 622, the program body 6221, the public key 6222, and the private key 6224 are created as one.

[0159] If drawing 12 is referred to, processing of the inclusion function part 611 of the pocket device 61 and the inclusion function part 621 of the main phone machine 62 will consist of the communication link demand generating step S601, the public key acquisition step S602, the mutual recognition step S603, the public key comparison step S604, mutual recognition and a public key coincidence judging step S605, a communication link authorization step S606, and a communication link disapproval step S607.

[0160] Next, actuation of the information system with which the program ID communication link range control approach concerning the gestalt of the 6th operation constituted in this way was applied is explained to a detail with reference to drawing 11 and drawing 12.

[0161] When a communication link demand occurs between the process 6120 which performs the program 612 in the pocket device 61, and the process 6220 which performs the program 622 in the main phone machine 62 (step S601), First, the inclusion function part 611 of the pocket device 61 The public key 6122 showing the source origin of the program 612 which becomes the inclusion function part 621 of the main phone machine 62 the origin of a process 6120 the inclusion function part 621 of delivery and the main phone machine 62 It investigates whether a public key 6122 and a public key 6222 are in agreement on delivery (step S602), next both sides in the public key 6222 showing the source origin of the program 622 which becomes the inclusion function part 611 of the pocket device 61 the origin of a process 6220 (step S603).

[0162] Next, mutual recognition of a program 612 and a program 622 is performed between the inclusion function part 611 of the pocket device 61, and the inclusion function part 621 of the main phone machine 62 (step S604).

[0163] For example, when the one-time password method by the public key of RSA is used, The inclusion function part 611 of the pocket device 61 a random character string to the inclusion function part 621 of the main phone machine 62 Delivery ("Challenge"), The inclusion function part 621 of the main phone machine 62 enciphers the character string with the private key 6224 of a program 622, and returns it to the inclusion function part 611 of the pocket device 61 ("Response"). The inclusion function part 611 of the pocket device 61 decodes the enciphered character string with a public key 6222, and if the decoded character string and the random character string sent previously are in agreement It attests with the program 622 which becomes the origin of a process 6220 having a public key 6222 (that is, the program 622 which becomes the origin of a process 6220 having a public key 6222 and the private key 6224 which makes a pair).

[0164] On the other hand, the inclusion function part 621 of the main phone machine 62 a random character string to the inclusion function part 611 of the pocket device 61 Delivery ("Challenge"), The inclusion function part 611 of the pocket device 61 enciphers the character string with the private key 6124 which accompanies the pocket device 61, and returns it to the inclusion function part 621 of the main phone machine 62 ("Response"). The inclusion function part 621 of the main phone machine 62 decodes the enciphered character string with a public key 6122, and if the decoded character string and the random character string sent previously are in agreement It attests with the program 612 which becomes the origin of a process 6120 having a public key 6122 (that is, the program 612 which becomes the origin of a process 6120 having a public key 6122 and the private key 6124 which makes a pair).

[0165] When the mutual recognition of a program 611 and a program 612 is successful and a

public key 6122 and a public key 6222 are in agreement (step S605), the inclusion function part 611 of the pocket device 61 and the inclusion function part 621 of the main phone machine 62 permit a communication link between a process 61210 and a process 62210 (step S606).

[0166] On the contrary, when the mutual recognition of a program 611 and a program 612 goes wrong, or when the public key 6122 showing the source origin of a program 612 and the public key 6222 showing the source origin of a program 622 are not in agreement, the inclusion function part 611 of the pocket device 61 and the inclusion function part 621 of the main phone machine 62 make a communication link disapproval between a process 6120 and a process 6220 (step S607).

[0167] According to the gestalt of the 6th operation, the program 612 in the pocket device 61 and the program 622 in the main phone machine 62 Since it cannot communicate with the programs 612 and 622 which accompany the public keys 6122 and 6222 in agreement and cannot communicate with other programs of arbitration, The range where the information which the program 612 in the pocket device 61 and the program 622 in the main phone machine 62 have circulates can be restricted within the limits of the program which makes the source origin the same.

[0168] Moreover, since the program 612 in the pocket device 61 and the program 622 in the main phone machine 62 cannot communicate with the programs 612 and 622 which accompany the public keys 6122 and 6222 in agreement and cannot communicate with other programs of arbitration, the information which the program 612 in the pocket device 61 and the program 622 in the main phone machine 62 have will not be revealed out of range [the program which makes the source origin the same], even if programs 612 and 622 overrun recklessly.

[0169] Furthermore, it is that the design in respect of [about control of the communication link range in a distributed environment] security becomes easy, and a degree of freedom does not change. The reason in order not to circulate information only between the programs which make the same the thing similar to the manufacturer or it about the information leak at the time of the communication link which is one of the important reasonable problems in a distributed environment Even if it does not design the circulation range of informational at the time of a design, neither the leakage to the malicious others nor the leakage by the bug of a program and overrun takes place, and it sets in one service conversely. Information can be circulated by regarding it as the thing similar to the one manufacturer or it which is the whole thing in connection with the project, and it is because it is enough in the circulation range.

[0170] (7) If gestalt drawing 13 of the 7th operation is referred to, the information system with which the program ID communication link range control approach concerning the gestalt of operation of the 7th of this invention was applied The pocket device 71 which has a program execution function and communication facility, and the main phone machine 72 which similarly has a program execution function and communication facility, The principal part consists of a program 712 which is installed in the pocket device 71 and performed, and a program 722 which is installed in the main phone machine 72 and performed.

[0171] As for an execution function and communication facility, Java etc. is assumed.

[0172] As a pocket device 71, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0173] A POS terminal etc. is assumed as a main phone machine 72.

[0174] The communication mode used for the communication facility between the pocket device 71 and the main phone machine 72 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0175] The pocket device 71 is constituted including the reliable inclusion function part 711, the process 7120 which performs a program 712, the private key 7131 and public key 7132 which accompany the pocket device 71, and the public key 7232 which accompanies the main phone machine 72.

[0176] The program 712 is constituted including the hash value 7123 which is the signature which enciphered the public key 7122 and the pair with the private key (not shown) to make in the program body 7121, the public key 7122 showing the source origin of a program 712, and the digest that carried out hashing of the program body 7121 by the Hash Function. In addition, in

the sources (manufacturer etc.) and origins (version etc.), as for the program 712, the program body 7121, the public key 7122, and the hash value 7123 are created as one.

[0177] The main phone machine 72 is constituted including the reliable inclusion function part 721, the process 7220 which performs a program 722, the private key 7231 and public key 7232 which accompany the main phone machine 72, and the public key 7132 which accompanies the pocket device 71.

[0178] The program 722 is constituted including the hash value 7223 which is the signature which enciphered the public key 7222 and the pair with the private key (not shown) to make in the program body 7221, the public key 7222 showing the source origin of a program 722, and the digest that carried out hashing of the program body 7221 by the Hash Function. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 722, the program body 7221, the public key 7222, and the hash value 7223 are created as one.

[0179] If drawing 14 is referred to, processing of the inclusion function part 711 of the pocket device 71 and the inclusion function part 721 of the main phone machine 72 will consist of the hash value check steps S701 and S702, the communication link demand generating step S703, the mutual recognition step S704, the public key coincidence judging step S705, a communication link authorization step S706, and a communication link disapproval step S707.

[0180] Next, actuation of the information system with which the program ID communication link range control approach concerning the gestalt of the 7th operation constituted in this way was applied is explained to a detail with reference to drawing 13 and drawing 14.

[0181] First, the pocket device 71 checks whether a hash value 7123 is generated by the program body 7121 and the public key group 7122 and a public key 7122, and the private key that makes a pair by the inclusion function part 711 (step S701). While obtaining the digest which the inclusion function part 711 decoded the hash value 7123 with the public key 7122, and carried out hashing of the program body 7221 in detail, it is verifying whether hashing of the program body 7121 being carried out by the known Hash Function, a digest's being obtained, and both digests being completely in agreement, and a hash value 7123 checks whether it is generated by the program body 7121 and the public key group 7122 and a public key 7122, and the private key that makes a pair. That is, the program body 7121 and a public key 7122 were not altered, and it checks that a program 712 has the Shinsei source origin. In addition, this check processing should just be performed once, when a program 712 introduced for example, downloads to the pocket device 71.

[0182] Moreover, the main phone machine 72 also checks whether a hash value 7223 is generated by the program body 7221 and the public key group 7222 and a public key 7222, and the private key that makes a pair by the inclusion function part 721 (step S702). While obtaining the digest which the inclusion function part 721 decoded the hash value 7223 with the public key 7222, and carried out hashing of the program body 7221 in detail, it is verifying whether hashing of the program body 7221 being carried out by the known Hash Function, a digest's being obtained, and both digests being completely in agreement, and a hash value 7223 checks being generated with the program body 7221 and the public key group 7222 and a public key 7222, and the private key that makes a pair. That is, the program body 7221 and a public key 7222 were not altered, and it checks that a program 722 has the Shinsei source origin. In addition, this check processing should just be performed once, when a program 722 is introduced for example, installed in the main phone machine 72.

[0183] Next, when the process 7120 which performs the program 712 in the pocket device 71, and the process 7220 which performs the program 722 in the main phone machine 72 tended to communicate and a communication link demand occurs (step S703), Before it, first or between the inclusion function part 711 of the pocket device 71, and the inclusion function part 721 of the main phone machine 72 The public key system using the private key 7131 and public key 7132 with which the pocket device 71 accompanies, and the private key 7231 and public key 7232 which accompany the main phone machine 72 performs mutual recognition of the pocket device 71 and the main phone machine 72 (step S704).

[0184] For example, it judges whether the public key 7132 which accompanies the pocket device 71 held as a public key in which the partner with whom oneself may communicate is shown, and

the public key 71132 of the main phone machine 72 which accompanies the pocket device 71 which the pocket device 71 holds correspond, and when in agreement, the pocket device 71 is attested. On the other hand, it judges whether the public key 7232 which accompanies the main phone machine 72 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 72132 of the pocket device 71 which accompanies the main phone machine 72 which the main phone machine 72 holds correspond, and when in agreement, the main phone machine 72 is attested.

[0185] Moreover, when the one-time password method by the public key of RSA is used, The inclusion function part 711 of the pocket device 71 a random character string in the main phone vessel 72 Delivery ("Challenge"), The inclusion function part 721 of the main phone machine 72 enciphers the character string with the private key 7231 which accompanies the main phone machine 72, and returns it to the pocket device 71 ("Response"). If the inclusion function part 711 of the pocket device 71 decodes the enciphered character string with the public key 7232 which accompanies the main phone machine 72 and the decoded character string and its random character string sent previously correspond The main phone machine 72 is attested with his being the partner (that is, thing which owns the public key 7232 which accompanies the main phone machine 72, and the private key 7231 which makes a pair) who may communicate. On the other hand, the inclusion function part 721 of the main phone machine 72 a random character string to the pocket device 71 Delivery ("Challenge"), The inclusion function part 711 of the pocket device 71 enciphers the character string with the private key 7131 which accompanies the pocket device 71, and returns it to the main phone machine 72 ("Response"). The inclusion function part 721 of the main phone machine 72 decodes the enciphered character string with the public key 7132 which accompanies the pocket device 71. If the decoded character string and the random character string sent previously are in agreement, the pocket device 71 will be attested with his being the partner (that is, thing which owns the public key 7132 which accompanies the pocket device 71, and the private key 7131 which makes a pair) who may communicate.

[0186] When it succeeds in mutual recognition, it judges whether the public key 7122 with which the inclusion function part 711 of the pocket device 71 and the inclusion function part 721 of the main phone machine 72 express the source origin of a program 712, and the public key 7222 showing the source origin of a program 722 are transmitted to a partner at each other, and both public keys are in agreement (step S705), when in agreement, it restricts, and a communication link is permitted between a process 71210 and a process 72210 (step S706).

[0187] When the mutual recognition of the pocket device 71 and a main phone 72 goes wrong (step S704), or when the public key 7122 showing the source origin of a program 712 and the public key 7222 showing the source origin of a program 722 are not in agreement (step S705), the inclusion function part 711 of the pocket device 71 and the inclusion function part 721 of the main phone machine 72 make disapproval the communication link between a process 7120 and a process 7220 (step S707).

[0188] According to the gestalt of the 7th operation, the program 712 in the pocket device 71 and the program 722 in the main phone machine 72 Since it cannot communicate with the programs 712 and 722 which accompany the public keys 7122 and 7222 in agreement and cannot communicate with other programs of arbitration, The range where the information which the program 712 in the pocket device 71 and the program 722 in the main phone machine 72 have circulates can be restricted within the limits of the program which makes the source origin the same.

[0189] Moreover, since the program 712 in the pocket device 71 and the program 722 in the main phone machine 72 cannot communicate with the programs 712 and 722 which accompany the public keys 7122 and 7222 in agreement and cannot communicate with other programs of arbitration, the information which the program 712 in the pocket device 71 and the program 722 in the main phone machine 72 have will not be revealed out of range [the program which makes the source origin the same], even if programs 712 and 722 overrun recklessly.

[0190] Furthermore, it is that the design in respect of [about control of the communication link range in a distributed environment] security becomes easy, and a degree of freedom does not

change. The reason in order not to circulate information only between the programs which make the same the thing similar to the manufacturer or it about the information leak at the time of the communication link which is one of the important reasonable problems in a distributed environment Even if it does not design the circulation range of informational at the time of a design, neither the leakage to the malicious others nor the leakage by the bug of a program and overrun takes place, and it sets in one service conversely. Information can be circulated by regarding it as the thing similar to the one manufacturer or it which is the whole thing in connection with the project, and it is because it is enough in the circulation range.

[0191] Even if programs 712 and 722 do not have a private key, furthermore, the pocket device 71 and a main phone 72 From the process 7220 in a partner and authentication of the programs 722 and 712 which become the origin of 7120** being possible When communicating with the partner who does based on the programs 712 and 722 which steal and are under the environment in which a **** alteration is possible, and operates, the pocket device 71 and the main phone machine 72 can prevent ***** of programs 722 and 712, and it can attest.

[0192] (8) If gestalt drawing 15 of the 8th operation is referred to, the information system with which the channel offer approach was applied the program ID communication link range control approach concerning the gestalt of operation of the 8th of this invention, and the whole public key In the information system with which the program ID communication link range control approach concerning the gestalt of the 7th operation was applied The pocket device 81 and the main phone machine 82 further Communication devices 815 and 825, The virtual sockets 81511-8151i, and 82611-8251j which can assign all port numbers for every public key, that is, may exist for every public key value by the same port number, It is constituted including Sockets 81521-8152k and 82521-8252l. In addition, the sign which changed the initial character "7" of a sign into "8" is given to the part in the information system with which the program ID communication link range control approach concerning the gestalt of the 7th operation was applied, and a corresponding part, and those detailed explanation is omitted.

[0193] What made other channels, such as a channel and a pipe, virtual is sufficient as the virtual sockets 81511-8151i, and 82611-8251j, and they may be other channels, such as Sockets 81521-8152k and 82521-8252l., a channel, and a pipe.

[0194] If drawing 16 is referred to, processing of the inclusion function part 811 of the pocket device 81 and the inclusion function part 821 of the main phone machine 82 will consist of the hash value check steps S801 and S802, the communication link demand generating step S803, the mutual recognition step S804, the public key coincidence judging step S805, a communication link authorization step S806, and a communication link disapproval step S807.

[0195] Next, actuation of the information system with which the program ID communication link range control approach concerning the gestalt of the 8th operation constituted in this way was applied is explained to a detail with reference to drawing 15 and drawing 16.

[0196] Step S801 - step S805, and step S807 are the same as step S701 - step S705, and step S707 in the program ID communication link range control approach concerning the gestalt of the 7th operation.

[0197] In actuation of the information system with which the program ID communication link range control approach concerning the gestalt of the 7th operation was applied It restricts, when in agreement [in step S806 which permits a communication link] between a process 8120 and a process 8220. Communication devices 815 and 825 As opposed to the pair of the port number of the virtual socket which public keys 8122 and 8222, a process 81210, and a process 82210 require, respectively One of the virtual channels formed in the channel with the socket which incorporates with the inclusion function part 811 and is used between function parts 821 is assigned, and the communication link between a process 81210 and a process 82210 is permitted according to this virtual channel.

[0198] (9) If gestalt drawing 17 of the 9th operation is referred to, the information system with which the program ID communication link range control approach concerning the gestalt of operation of the 9th of this invention was applied The pocket device 91 which has a program execution function and communication facility, and the main phone machine 92 which similarly has a program execution function and communication facility, The principal part consists of a

program 912 which is installed in the pocket device 91 and performed, and a program 922 which is installed in the main phone machine 92 and performed.

[0199] As for an execution function and communication facility, Java etc. is assumed.

[0200] As a pocket device 91, a portable telephone (PHS is included), a Personal Digital Assistant, etc. are assumed.

[0201] A POS terminal etc. is assumed as a main phone machine 92.

[0202] The communication mode used for the communication facility between the pocket device 91 and the main phone machine 92 shall be realized by short-distance radio techniques, such as Bluetooth which Ericsson advocates, wireless LAN, and PIAFS.

[0203] The pocket device 91 is constituted including the reliable inclusion function part 911, the process 9120 which performs a program 912, the private key 9131 and public key 9132 which accompany the pocket device 91, and the public key 9232 which accompanies the main phone machine 92.

[0204] The program 912 is constituted including the hash value groups 91231-9123n which are signature groups which enciphered the digest which carried out hashing of the data created combining the program body 9121, the public key groups 91221-9122n showing the source origin of a program 912, and the program body 9121 and the public key groups 91221-9122n by the Hash Function with each public keys 91221-9122n and each private key (not shown) which makes a pair. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 912, the program body 9121, the public key groups 91221-9122n, and the hash value groups 91231-9123n are created as one.

[0205] The main phone machine 92 is constituted including the reliable inclusion function part 921, the process 9220 which performs a program 922, the private key 9231 and public key 9232 which accompany the main phone machine 92, and the public key 9132 which accompanies the pocket device 91.

[0206] Programs 922 are the public key groups 92221-9222m (m is a positive integer on two.) which express the source origin of a program 922 as the program body 9221. It is constituted including that it is the same as that of the following, and the hash value groups 92231-9223m which are signature groups which enciphered the digest which carried out hashing of the data constituted by the program body 9221 and the public key groups 92221-9222m by the Hash Function with each public keys 92221-9222m and each private key (not shown) which makes a pair. In addition, in the sources (manufacturer etc.) and origins (version etc.), as for the program 922, the program body 9221, the public key groups 92221-9222m, and the hash value groups 92231-9223m are created as one.

[0207] If drawing 18 is referred to, processing of the inclusion function part 911 of the pocket device 91 and the inclusion function part 921 of the main phone machine 92 will consist of the hash value check steps S901 and S902, the communication link demand generating step S903, the mutual recognition step S904, the public key coincidence judging step S905, a communication link authorization step S906, and a communication link disapproval step S907.

[0208] Next, actuation of the information system with which the program ID communication link range control approach concerning the gestalt of the 9th operation constituted in this way was applied is explained to a detail with reference to drawing 17 and drawing 18.

[0209] First, the pocket device 91 obtains the assembly of the public key corresponding to the hash value which each hash values 91231-9123n checked whether it would be generated by the program body 9121 and the public key groups 91221-9122n, each public keys 91221-9122n, and each private key that makes a pair, and checked by the inclusion function part 911 (step S901). In detail the inclusion function part 911 While obtaining the digest group which carried out hashing of the data which decoded each hash values 91231-9123n with each public keys 91221-9122n, respectively, and were created combining the program body 9121 and the public key groups 91221-9122n Carry out hashing of the data created combining the program body 9121 and the public key groups 91221-9122n by the known Hash Function, and a digest is obtained. By verifying, respectively, whether each of this digest and digest groups is completely in agreement It checks, respectively that each hash values 91231-9123n are generated with the program body 9121 and the public key groups 91221-9122n, each public keys 91221-9122n, and

each private key that makes a pair. The assembly of the public key corresponding to the checked hash value is obtained. That is, the program body 9121 and at least one or more public keys in 91221-9122n of public key groups were not altered, and it checks having the Shinsei source origin. In addition, this check processing should just be performed once, when a program 912 introduced for example, downloads to the pocket device 91.

[0210] Moreover, the inclusion function part 921 obtains the assembly of the public key corresponding to the hash value to which each hash values 92231-9223n also checked and checked the pocket device 92 for whether it is generated by the program body 9221 and the public key groups 92221-9222n, each public keys 92221-9222n, and each private key (not shown) that makes a pair (step S902). In detail the inclusion function part 921 While obtaining each digest which carried out hashing of the data which decoded each hash values 92231-9223m with public keys 92221-9222m, respectively, and were created combining the program body 9221 and the public key groups 92221-9222m The digest which carried out hashing of the data created combining the program body 9221 and the public key groups 92221-9222m by the known Hash Function is obtained. By verifying, respectively, whether both the ** digest is completely in agreement It checks, respectively that each hash values 92231-9223n are generated with the program body 9221 and the public key groups 92221-9222n, each public keys 92221-9222n, and each private key (not shown) that makes a pair. The assembly of the public key corresponding to the checked hash value is obtained. That is, the program body 9221 and at least one or more public keys in 92221-9222m of public key groups were not altered, and it checks having the Shinsei source origin. In addition, this check processing should just be performed once, when a program 922 is introduced for example, installed in the main phone machine 92.

[0211] Next, when the process 9120 which performs the program 912 in the pocket device 91, and the process 9220 which performs the program 922 in the main phone machine 92 tended to communicate and a communication link demand occurs (step S903), Before it, first or between the inclusion function part 911 of the pocket device 91, and the inclusion function part 921 of the main phone machine 92 The public key system using the private key 9131 and public key 9132 which accompany the pocket device 91, and the private key 9231 and public key 9232 which accompany the main phone machine 92 performs mutual recognition (step S904).

[0212] For example, it judges whether the public key 9132 which accompanies the pocket device 91 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 91132 of the main phone machine 92 which accompanies the pocket device 91 which the pocket device 91 holds correspond, and when in agreement, the pocket device 91 is attested. On the other hand, it judges whether the public key 9232 which accompanies the main phone machine 92 held as a public key in which the partner with whom oneself may communicate is shown, and the public key 92132 of the pocket device 91 which accompanies the main phone machine 92 which the main phone machine 92 holds correspond, and when in agreement, the main phone machine 92 is attested.

[0213] Moreover, when the one-time password method by the public key of RSA is used, The inclusion function part 911 of the pocket device 91 a random character string in the main phone vessel 92 Delivery ("Challenge"), The inclusion function part 921 of the main phone machine 92 enciphers the character string with the private key 9231 which accompanies the main phone machine 92, and returns it to the pocket device 91 ("Response"). If the inclusion function part 911 of the pocket device 91 decodes the enciphered character string with the public key 9232 which accompanies the main phone machine 92 and the decoded character string and its random character string sent previously correspond The main phone machine 92 is attested with his being the partner (that is, thing which owns the public key 9232 which accompanies the main phone machine 92, and the private key 9231 which makes a pair) who may communicate. On the other hand, the inclusion function part 921 of the main phone machine 92 a random character string to the pocket device 91 Delivery ("Challenge"), The inclusion function part 911 of the pocket device 91 enciphers the character string with the private key 9131 which accompanies the pocket device 91, and returns it to the main phone machine 92 ("Response"). If the inclusion function part 921 of the main phone machine 92 decodes the enciphered character string with the public key 9132 which accompanies the pocket device 91 and the decoded character string

and its random character string sent previously correspond. The pocket device 91 is attested with his being the partner (that is, thing which owns the public key 9132 which accompanies the pocket device 91, and the private key 9131 which makes a pair) who may communicate.

[0214] When it succeeds in mutual recognition, it judges whether the inclusion function part 911 of the pocket device 91 and the inclusion function part 921 of the main phone machine 92 tell each other the assembly of the public key of a hash value check result at a partner, and have a public key in agreement (step S905), in a certain case, one or more public keys in agreement restrict it, and a communication link is permitted between a process 91210 and a process 92210 (step S906).

[0215] When the mutual recognition of the pocket device 91 or a main phone 92 goes wrong at step S904, or when one does not have the public key which is in agreement at step S905, the inclusion function part 911 of the pocket device 91 and the inclusion function part 921 of the main phone machine 92 make disapproval the communication link between a process 9120 and a process 9220 (step S907).

[0216] in addition, with the gestalt of implementation of the above 9th. Although it judged with it being that in which programs 912 and 922 have the Shinsei source origin when one or more public keys which are in agreement with the assembly of the public key of the hash value check result by the pocket device 91 and the assembly of the public key of a hash value check result with the main phone machine 92 at step S905 were contained. Only when all the public keys of the assembly of the public key of the hash value check result by the pocket device 91 and the assembly of the public key of a hash value check result with the main phone machine 92 are in agreement, a communication link can be permitted between a process 91210 and a process 92210.

[0217] According to the gestalt of the 9th operation, since the hash value groups 91231-9123n which are signature groups, and 92231-9223n are attached to the public key groups 91221-9122n held with the program bodies 9121 and 9221, and 92221-9222n when allowing programs 912 and 922 to have the public key groups 91221-9122n showing the source origin of these programs 912 and 922, and 92221-9222n, ***** of programs 512 and 522 can be prevented.

[0218]

[Effect of the Invention] The 1st effectiveness is being able to prevent ***** and being able to attest the program of a communications partner, when performing the equipment and the communication link which carry out based on the program which an external device steals and has it under the environment in which a **** alteration is possible, and operate. The reason is that it can attest without a program's having a private key.

[0219] The 2nd effectiveness is being able to allow having the public key which a program's prevents ***** and expresses two or more source origins. The reason is that it signs to the public key group held with the program body when allowing having a public key showing two or more source origins.

[0220] The 3rd effectiveness is being able to maintain security to a malicious program. The reason is that it communicates by ID showing the source origin of a program, i.e., the access control carried out based on the information similar to the manufacturer and the version of a program.

[0221] The 4th effectiveness is being able to maintain the security about processing by the communication link under the distributed environment which does not need a centralized control system like user management. The reason is that it can maintain security to a malicious program since it communicates by ID showing the source origin of a program, i.e., the access control carried out based on the information similar to the manufacturer and the version of a program.

[0222] The 5th effectiveness is restricted within the limits of the program to which the range where the information which the program in program execution and a communication device has circulates makes the source origin the same. The reason is because the program in program execution and a communication device can communicate only with the program which has ID showing the source origin in agreement and cannot communicate with other programs of arbitration.

[0223] The 6th effectiveness is not revealing out of range [the program to which the information which the program in program execution and a communication device has will make the source origin the same even if a program overruns recklessly]. The reason is because the program in program execution and a communication device can communicate only with the program which has ID showing the source origin in agreement and cannot communicate with other programs of arbitration.

[0224] The 7th effectiveness is that the range where the information which the program in program execution and a communication device has circulates is restricted within the limits of the program which makes the source origin the same. The reason is possible [a communication link] only between the programs offered by the thing holding the same private key, when the program in program execution and a communication device uses ID showing the source origin in agreement as a public key.

[0225] The 8th effectiveness is that the design in respect of [about control of the communication link range in a distributed environment] security becomes easy, and a degree of freedom does not change. The reason in order not to circulate information only between the programs which make the source origin the same about the information leak at the time of the communication link which is one of the important reasonable problems in a distributed environment Even if it does not design the circulation range of informational at the time of a design, neither the leakage to the malicious others nor the leakage by the bug of a program and overrun takes place, and it sets in one service conversely. Information can be circulated by regarding it as the thing similar to the one manufacturer or it which is the whole thing in connection with the project, and it is because it is enough in the circulation range.

[0226] The 9th effectiveness is being able to maintain security to a malicious program. The reason is that it performs communication link propriety based on ID showing the source origin of a program, i.e., the information similar to the manufacturer and the version of a program.

[0227] The 10th effectiveness is being able to maintain the security about processing by the communication link under the distributed environment which does not need a centralized control system like user management. The reason is that it can maintain security to a malicious program since communication link propriety is performed based on ID showing the source origin of a program, i.e., the information similar to the manufacturer and the version of a program.

[0228] The 11th effectiveness is that the system design about a channel is easy, when performing the communication link according to public key. The reason is that it is limited beforehand which channel is occupied by which object for public keys.

[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-152196

(P 2 0 0 2 - 1 5 2 1 9 6 A)

(43) 公開日 平成14年5月24日 (2002.5.24)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
H04L 9/32		G09C 1/00	640 D 5J104
G09C 1/00	640		660 D 5K067
	660	H04L 9/00	675 B
H04Q 7/38		H04B 7/26	109 S

審査請求 有 請求項の数35 O L (全43頁)

(21) 出願番号 特願2001-250922 (P 2001-250922)

(22) 出願日 平成13年8月22日 (2001.8.22)

(31) 優先権主張番号 特願2000-264850 (P 2000-264850)

(32) 優先日 平成12年9月1日 (2000.9.1)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72) 発明者 市瀬 規善
東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100088890
弁理士 河原 純一

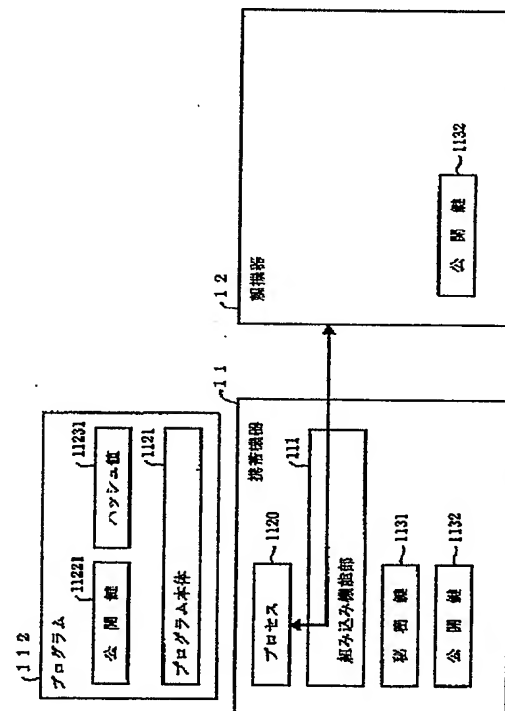
Fターム(参考) 5J104 AA07 AA08 AA09 KA02 KA05
KA21 LA03 LA05 LA06 NA02
NA12 PA02
5K067 AA32 BB04 DD17 DD23 EE02
EE10 HH22 HH23 HH24

(54) 【発明の名称】 秘密鍵なしプログラム認証方法、プログラムID通信処理制御方法、プログラムID通信範囲制御方法および公開鍵毎通信路提供方法

(57) 【要約】

【課題】 読み出し改竄可でよい環境での、通信における成りすましを防止する。

【解決手段】 携帯機器11が、組み込み機能部111により、ハッシュ値11231がプログラム本体1121とプログラム112の出所由来を表す公開鍵11221と対をなす秘密鍵とによって生成されたものであることを確認する。親機器12が、公開鍵11232および秘密鍵1131を用いた公開鍵方式により携帯機器11の認証を行い、認証が成功した場合に、携帯機器11によるハッシュ値確認結果に基づいてプログラム112が真正な出所由来をもつものを判定する。親機器12が携帯機器11の認証に成功し、かつプログラム112が真正な出所由来をもつものであるときに、公開鍵11221でプログラム112を認証したとする。



【特許請求の範囲】

【請求項 1】 プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が該公開鍵を前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする秘密鍵なしプログラム認証方法。

【請求項 2】 前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項 1 記載の秘密鍵なしプログラム認証方法。

【請求項 3】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公

開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする請求項 1 または 2 記載の秘密鍵なしプログラム認証方法。

【請求項 4】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項 1 または 2 記載の秘密鍵なしプログラム認証方法。

【請求項 5】 プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が 1 つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の各公開鍵を、前記プログラムの出所由来を表すと認証する工程とを含むこと

を特徴とする秘密鍵なしプログラム認証方法。

【請求項 6】 前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認した署名に対応する公開鍵の集まりを得る工程において、各署名が前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする請求項 5 記載の秘密鍵なしプログラム認証方法。

【請求項 7】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする請求項 5 または 6 記載の秘密鍵なしプログラム認証方法。

【請求項 8】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項 5 または 6 記載の秘密鍵なしプログラム認証方法。

【請求項 9】 プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す ID 群とを含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プロ

ラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プロセスの元となるプログラムの出所由来を表す ID 群の一部または全部を得る工程と、前記出所由来を表す ID が 1 つ以上得られたときに、前記通信・処理装置が前記プログラムを元に生成されたプロセスの処理により前記プログラム実行・通信装置と通信を行う工程と、通信によって発生した処理において、前記通信・処理装置が、前記プログラム実行・管理装置から得られた前記出所由来を表す ID 群を元にしたアクセス制御を行う工程とを含むことを特徴とするプログラム ID 通信処理制御方法。

【請求項 10】 プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体、該プログラムの出所由来を表す公開鍵、および該公開鍵と対をなす秘密鍵を含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置から該プログラム実行・通信装置に通信をさせるプロセスの元となる前記プログラムの出所由来を表す公開鍵を得る工程と、前記通信・処理装置が、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程と、前記プログラムが認証されたときに、前記通信・処理装置が、前記公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラム ID 通信処理制御方法。

【請求項 11】 前記通信・処理装置が、得られた公開鍵について、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記プログラム実行・通信装置が、前記公開鍵を前記通信・処理装置に送り、前記通信・処理装置が、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置が、該文字列を前記秘密鍵で暗号化した文字列を前記通信・処理装置に送り返し、前記通信・処理装置が、暗号化された文字列を前記送られてきた公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラムを認証することを特徴とする請求項 10 記載のプログラム ID 通信処理制御方法。

【請求項 12】 プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プロ

グラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置から前記プログラムの出所由来を表す公開鍵を得、該公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムID通信処理制御方法。

【請求項13】 前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項12記載のプログラムID通信処理制御方法。

【請求項14】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする請求項12または13記載のプログラムID通信処理制御方法。

【請求項15】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項12または13記載のプログラムID通信処理制御方法。

【請求項16】 プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が1つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の公開鍵の集まりの一部または全部を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とするプログラムID通信処理制御方法。

【請求項17】 前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合

わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせることで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を各公開鍵でそれぞれ復号した各ダイジェストと、前記プログラム本体および前記公開鍵群を組み合わせることで作成されたデータをハッシュ関数でハッシングして得られるダイジェストとが一致するかどうかを判定することを特徴とする請求項 16 記載のプログラム ID 通信処理制御方法。

【請求項 18】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする請求項 16 または 17 記載のプログラム ID 通信処理制御方法。

【請求項 19】 前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする請求項 16 または 17 記載のプログラム ID 通信処理制御方法。

【請求項 20】 プログラムと、これらプログラムを元にプロセスをそれぞれ生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体、および該プログラムの出所由来を表す ID 群を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す ID 群の一部または全部を得る工程と、前記出所由来を表す ID 群が得られたときに、両プログラム実行・通信装置が、得られた出所由来を表す ID 群と自プログラム実行・通信装

置内のプロセスの元となる前記プログラムの出所由来を表す ID 群とを比較し、一致する前記プログラムの出所由来を表す ID が 1 つ以上存在すれば通信路を開く工程とを含むことを特徴とするプログラム ID 通信範囲制御方法。

【請求項 21】 プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体、該プログラムの出所由来を表す公開鍵、および該公開鍵と対をなす秘密鍵を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置から相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵をそれぞれ得る工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程と、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致し、かつ相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証されたときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とするプログラム ID 通信範囲制御方法。

【請求項 22】 両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、両プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵を相手プログラム実行・通信装置に送り、相手プログラム実行・通信装置にランダムな文字列をそれぞれ送り、相手プログラム実行・通信装置が、該文字列を相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した文字列を自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置が、暗号化された文字列を対応する公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置通信装置内のプロセスの元となるプ

プログラムを認証することとを特徴とする請求項 2 1 記載のプログラム I D 通信範囲制御方法。

【請求項 2 3】 プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記通信を行う前に、前記公開鍵を相手プログラム実行・通信装置に伝える工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証され、かつ相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致したときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とするプログラム I D 通信範囲制御方法。

【請求項 2 4】 両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、両プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする請求項 2 3 または 2 4

記載のプログラム I D 通信範囲制御方法。

【請求項 2 5】 両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の 1 つ以上の公開鍵とが一致するかどうかを判定することを特徴とする請求項 2 3 または 2 4 記載のプログラム I D 通信範囲制御方法。

【請求項 2 6】 両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする請求項 2 3 または 2 4 記載のプログラム I D 通信範囲制御方法。

【請求項 2 7】 両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路 1 つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の 1 つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする請求項 2 6 記載のプログラム I D 通信範囲制御方法。

【請求項 2 8】 プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、各プログラムを元に生成および実行されるプロセスとを含み、各プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を

組み合わせで作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせで作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりを相手プログラム実行・通信装置に伝え、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりと相手プログラム実行・通信装置による署名確認結果の公開鍵の集まりとに一致する公開鍵があるかどうかを判定する工程と、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵が1つ以上あるときに、両プログラム実行・通信装置が、プロセス間の通信路を開く工程とを含むことを特徴とするプログラムID通信範囲制御方法。

【請求項29】 両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせで作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを判定する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、相手プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群で作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする請求項28記載のプログラムID通信範囲制御方法。

【請求項30】 両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の1つ以上の公開鍵とが一致するかどうかを判定することを特徴とする請求項28または29記載のプログラムID通信範囲制御方法。

【請求項31】 両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タ

イム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする請求項28または29記載のプログラムID通信範囲制御方法。

【請求項32】 両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が1つ以上得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の1つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする請求項31記載のプログラムID通信範囲制御方法。

【請求項33】 仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする請求項27または32記載のプログラムID通信範囲制御方法。

【請求項34】 プログラムと、該プログラムを元にプロセスを生成し実行および通信するプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に1つ以上存在する仮想通信路用資源と、1つ以上の通信路用資源とを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により通信を行う際に、出所由来を表す公開鍵と要求された仮想通信路用資源とを対にして仮想通信路と対応させ、仮想通信路を使い通信路を提供する工程を含むことを特徴とする公開鍵毎通信路提供方法。

【請求項 35】 仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする請求項 34 記載の公開鍵毎通信路提供方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はプログラム認証方法、分散環境におけるプログラム間通信により発生する処理のアクセス制御方法、および分散環境におけるプログラムの通信範囲制御方法に関する。

【0002】

【従来の技術】 従来の情報システムの一例は、たとえば図 19 に示すように、プログラム本体 10121、およびプログラム 1012 の出所由来を表す公開鍵群 101221~10122n と秘密鍵群 101241~10124n との対により構成されるプログラム 1012 と、プログラム実行・通信装置である携帯機器 101 によりプログラム 1012 を元に生成および実行されるプロセス 10120 により構成される、プログラム 1012 を対象としプログラム 1012 を元にプロセス 10120 を生成し実行する携帯機器 101 と、携帯機器 101 と通信を行う通信・処理装置である親機器 102 とにより、その主要部が構成されていた。

【0003】 従来の情報システムの一例は、たとえば図 19 に示すように、プログラム 1012 と、プログラム 1012 を元にプロセス 10120 を生成し実行するプログラム実行・通信装置である携帯機器 101 と、携帯機器 101 と通信を行う通信・処理装置である親機器 102 とから、その主要部が構成されていた。

【0004】 プログラム 112 は、プログラム本体 10121 と、プログラム 1012 の出所由来を表す公開鍵群 101221~10122n と、公開鍵群 101221~10122n と対をなす秘密鍵群 101241~10124n とを含んで構成されていた。

【0005】 携帯機器 101 は、組み込み機能部 1011 と、プログラム 1012 を実行するプロセス 10120 と、携帯機器 101 に付随する公開鍵 10132 と、公開鍵 10132 と対をなす秘密鍵 10131 と、ユーザ・パスワード情報 10190 とから構成されていた。

【0006】 親機器 102 は、通信してよい相手を表す ID である携帯機器 101 に付随する公開鍵 10132 と、通信してよいユーザを表すユーザ・パスワード情報 10190 とを含んで構成されていた。

【0007】 このような従来の情報システムでは、プログラム 1012 を元に生成されたプロセス 10120 の処理により携帯機器 101 が親機器 102 と通信を行う以前に、親機器 102 が、携帯機器 101 から携帯機器 101 に通信をさせるプロセス 10120 の元となるプ

ログラム 1012 の出所由来を表す公開鍵 101221~10122n を得る工程と、親機器 102 が、得られた各公開鍵 101221~10122n について、携帯機器 101 に通信をさせるプロセス 10120 の元となるプログラム 1012 の出所由来を表す公開鍵群 101221~10122n および秘密鍵群 101241~10124n を用いさせて認証を行うことで、プロセス 10120 の元となるプログラム 1012 が認証に成功した公開鍵すべてをもつと認証を行っていた。

【0008】 また、従来、情報システムの他の例は、たとえば図 20 に示すように、プログラム 1012 と、プログラム 1012 を元にプロセス 10120 を生成し実行するプログラム実行・通信装置である携帯機器 101 と、携帯機器 101 と通信を行う通信・処理装置である親機器 102 とから、その主要部が構成されていた。

【0009】 携帯機器 101 は、組み込み機能部 1011 と、プログラム 1012 を実行するプロセス 10120 と、携帯機器 101 に付随する公開鍵 10132 および秘密鍵 10131 と、ユーザ・パスワード情報 10190 とから構成されていた。

【0010】 親機器 102 は、通信してよい相手を示す公開鍵としての携帯機器 101 に付随する公開鍵 10132 と、ユーザ・パスワード情報 10190 とをもつ。

【0011】 このような従来の情報システムでは、携帯機器 101 で、ユーザ・パスワード情報 10190 について認証を行い、プログラム 1012 を実行するプロセス 10120 がユーザ・パスワード情報 10190 を保持する。プロセス 10120 が親機器 102 と通信をしようとして通信要求が発生した場合、親機器 102 は、携帯機器 101 から公開鍵 10132 を受け取り、公開鍵 10132 と一致するものであれば、携帯機器 101 に対し公開鍵 10132 について認証を行い、認証に成功した場合は、携帯機器 101 内のプログラム 1012 を実行するプロセス 10120 と親機器 102 との通信を許し、またその通信によって発生する処理についてのアクセス制御は、通信相手によらず同じアクセス制御を行うか、または通信相手のプロセス 10120 のもつユーザ・パスワード情報 10190 を引き継ぎ、ユーザ認証が成功すればそれをもとにアクセス制御を行っていた。

【0012】 さらに、従来、情報システムの別の例は、たとえば図 21 に示すように、携帯機器 101 と、親機器 102 とから、その主要部が構成されていた。

【0013】 携帯機器 101 は、組み込み機能部 1011 と、プログラム 1012 と、プログラム 1012 を実行するプロセス 10120 と、携帯機器 101 に付随する秘密鍵 10131 と、秘密鍵 10131 と対をなす公開鍵 10132 と、通信してよい相手を示す公開鍵 10232 とを含んで構成されていた。

【0014】 親機器 102 は、組み込み機能部 1021

と、プログラム 1022 と、プログラム 1022 を実行するプロセス 10220 と、親機器 102 に付随する秘密鍵 10231 と、秘密鍵 10231 と対を成す公開鍵 10232 と、通信してよい相手を示す公開鍵 10132 とから構成されていた。

【0015】このような従来の情報システムでは、プロセス 10120 とプロセス 10220 とが通信をしようとして通信要求が発生した場合、組み込み機能部 1011 および 1021 は、まず、公開鍵 10132 および 10232 を互いに渡し、受け取った公開鍵 10232 および 10132 と通信してよい相手を示す公開鍵 10232 および 10132 とをそれぞれ比較する。一致すれば、各組み込み機能部 1011 および 1021 は、受け取った公開鍵 10232 および 10132 で相互認証を行い、相互認証が成功すれば、プロセス 10120 とプロセス 10220 との通信を許す。一方、受け取った公開鍵 10232 および 10132 と通信してよい相手を示す公開鍵 10133 および 10233 とが異なるか、公開鍵 10232 および 10132 での相互認証が失敗した場合は、プロセス 10120 とプロセス 10220 との間の通信を許さなかった。また通信路資源群を仮想的に公開鍵毎に別資源として提供していなかった。

【0016】

【発明が解決しようとする課題】第 1 の問題点は、通信時の成りすましを防ぐためには、プログラムが存在するエリア（メモリ、ディスク等）のセキュリティレベルとして、読み出し改竄不可でなければならないということである。その理由は、プログラムが秘密鍵をもつ必要があるからである。

【0017】第 2 の問題点は、分散環境において、ユーザ・パスワード情報に類する共通の情報を保持し、維持管理する必要があることである。その理由は、認証するために同じユーザ・パスワード情報に類する情報を共有する必要があるからである。

【0018】第 3 の問題点は、ユーザ・パスワード情報に類する情報を利用しない場合は、通信相手によらず皆同じ権限で処理を実行させることである。その理由は、アクセス制御をするための正当性を保証できる情報を得られないからである。

【0019】第 4 の問題点は、機器、プログラムないしはシステムの設計時に機器、プログラムないしはプロセスの通信すべき相手をどのプログラムとするかを個別に設計しなければならないということである。その理由は、通信相手は通信すべき相手もっているはずの公開鍵の設定によって決まるからである。

【0020】第 5 の問題点は、システムの拡張および複数のシステムの乗り入れの際の手間が多いということである。その理由は、システムの拡張および複数のシステムの乗り入れのための、機器、プログラムないしはシステムの設計時に機器、プログラムないしはプロセスの通

信すべき相手をどのプログラムとするかを個々に設計し直さなければならないからである。

【0021】第 6 の問題点は、システムが特定のサービスに固定したものになりがちであることである。その理由は、システムの拡張および複数のシステムの乗り入れの際の手間が多いからである。

【0022】第 7 の問題点は、どの通信路をどの公開鍵に対応し利用するか設計、管理する必要があることである。その理由は、通信路資源群を仮想的に公開鍵毎に別資源として提供していなかったからである。

【0023】本発明の第 1 の目的は、プログラムが存在するエリアのセキュリティレベルとして、読み出し改竄可でよい環境での、通信における成りすましを防止する秘密鍵なしプログラム認証方法を提供することにある。

【0024】本発明の第 2 の目的は、集中管理下でない分散環境におけるプログラム間通信により発生する処理のアクセス制御を行うためのプログラム ID 通信処理制御方法を提供することにある。

【0025】本発明の第 3 の目的は、分散環境において、通信の範囲、つまり情報の流通について範囲が予め限定されており、通信範囲に関するシステム設計が容易なプログラム ID 通信範囲制御方法を提供することにある。

【0026】本発明の第 4 の目的は、公開鍵別の通信を行う場合に、どの通信路がどの公開鍵で占有されるかが予め限定されており、通信路に関するシステム設計が容易な公開鍵毎通信路提供方法を提供することにある。

【0027】なお、先行技術文献として特開 2000-148469 があるが、この公報に開示された「モジュラアプリケーション間のサービスへのアクセス制御」方法は、第 1 のコンピュータプログラムモジュールが第 2 のコンピュータプログラムモジュールからサービスのアクセスを与える権力をデジタル的に署名されたかどうかを判定し、デジタル的に署名された場合に第 1 のコンピュータプログラムモジュールにサービスへのアクセスを提供するようにしたものである。しかし、この方法は、第 1 のコンピュータプログラムモジュールが第 2 のコンピュータプログラムモジュールからのサービスにアクセスできるように、第 1 のコンピュータプログラムモジュールおよび第 2 のコンピュータプログラムモジュールを同じコンピューティングノード上の同じアドレス空間内で実行させることができるようにするためのものであり、本発明のように異なるプログラム実行・通信装置上で異なるプログラムを通信を介して協働させるようにするためのものではない。

【0028】

【課題を解決するための手段】本発明の秘密鍵なしプログラム認証方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処

理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が該公開鍵を前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする。

【0029】また、本発明の秘密鍵なしプログラム認証方法は、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【0030】さらに、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする。

【0031】さらにまた、本発明の秘密鍵なしプログラ

ム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【0032】また、本発明の秘密鍵なしプログラム認証方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせで作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせで作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が1つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の各公開鍵を、前記プログラムの出所由来を表すと認証する工程とを含むことを特徴とする。

【0033】さらに、本発明の秘密鍵なしプログラム認証方法は、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせ

10

20

30

40

50

作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認した署名に対応する公開鍵の集まりを得る工程において、各署名が前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群の組み合わせで作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする。

【0034】さらにまた、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と前記プログラム実行・通信装置に付随する公開鍵とが一致するかどうかを判定し、一致する場合に前記プログラム実行・通信装置を認証することを特徴とする。

【0035】また、本発明の秘密鍵なしプログラム認証方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【0036】一方、本発明のプログラムID通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体と、該プログラムの出所由来を表すID群とを含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プロセスの元となるプログラムの出所由来を表すID群の

一部または全部を得る工程と、前記出所由来を表すIDが1つ以上得られたときに、前記通信・処理装置が前記プログラムを元に生成されたプロセスの処理により前記プログラム実行・通信装置と通信を行う工程と、通信によって発生した処理において、前記通信・処理装置が、前記プログラム実行・管理装置から得られた前記出所由来を表すID群を元にしたアクセス制御を行う工程とを含むことを特徴とする。

【0037】また、本発明のプログラムID通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体、該プログラムの出所由来を表す公開鍵、および該公開鍵と対をなす秘密鍵を含み、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置から該プログラム実行・通信装置に通信をさせるプロセスの元となる前記プログラムの出所由来を表す公開鍵を得る工程と、前記通信・処理装置が、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程と、前記プログラムが認証されたときに、前記通信・処理装置が、前記公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【0038】さらに、本発明のプログラムID通信処理制御方法は、前記通信・処理装置が、得られた公開鍵について、前記プログラムの出所由来を表す公開鍵および秘密鍵を用いた公開鍵方式により前記プログラムの認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記プログラム実行・通信装置が、前記公開鍵を前記通信・処理装置に送り、前記通信・処理装置が、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置が、該文字列を前記秘密鍵で暗号化した文字列を前記通信・処理装置に送り返し、前記通信・処理装置が、暗号化された文字列を前記送られてきた公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラムを認証することを特徴とする。

【0039】さらにまた、本発明のプログラムID通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元

に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置から前記プログラムの出所由来を表す公開鍵を得、該公開鍵を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【0040】また、本発明のプログラムID通信処理制御方法は、前記プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、前記プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

【0041】さらに、本発明のプログラムID通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする。

【0042】さらにまた、本発明のプログラムID通信処理制御方法は、前記通信・処理装置が、前記プログラ

ム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【0043】また、本発明のプログラムID通信処理制御方法は、プログラムと、該プログラムを元にプロセスを生成し実行するプログラム実行・通信装置と、該プログラム実行・通信装置と通信を行う通信・処理装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、該プログラム実行・通信装置に付随する公開鍵および秘密鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵群と、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、生成されたものであることが確認された署名に対応する公開鍵の集まりを得る工程と、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程と、前記生成されたものであることが確認された署名に対応する公開鍵が1つ以上得られた場合に、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により前記通信・処理装置と通信を行う以前に、前記通信・処理装置が前記プログラムの出所由来を表す公開鍵を得る工程と、前記プログラム実行・通信装置の認証に成功し、かつ前記プログラムの出所由来を表す公開鍵を得られた場合に、前記通信・処理装置が、前記プログラム実行・通信装置による署名確認結果の公開鍵の集まりの一部または全部を元にしたアクセス制御により前記プログラム実行・通信装置と通信を行う工程とを含むことを特徴とする。

【0044】さらに、本発明のプログラムID通信処理制御方法は、前記プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせ

10

20

30

40

50

て作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、前記プログラム実行・通信装置が、各署名値を各公開鍵でそれぞれ復号した各ダイジェストと、前記プログラム本体および前記公開鍵群を組み合わせて作成されたデータをハッシュ関数でハッシングして得られるダイジェストとが一致するかどうかを判定することを特徴とする。

【0045】さらにまた、本発明のプログラムID通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、前記通信・処理装置が、通信してよい相手を示す公開鍵を備え、前記プログラム実行・通信装置に付随する公開鍵と前記通信してよい相手を示す公開鍵とが一致するかどうかを判定することを特徴とする。

【0046】また、本発明のプログラムID通信処理制御方法は、前記通信・処理装置が、前記プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により前記プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、前記通信・処理装置は、前記プログラム実行・通信装置にランダムな文字列を送り、前記プログラム実行・通信装置は、該文字列を該プログラム実行・通信装置に付随する秘密鍵で暗号化して前記通信・処理装置に送り返し、前記通信・処理装置は、暗号化された文字列を事前に保持する通信してよい相手を示す公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、前記プログラム実行・通信装置を認証することを特徴とする。

【0047】他方、本発明のプログラムID通信範囲制御方法は、プログラムと、これらプログラムを元にプロセスをそれぞれ生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体、および該プログラムの出所由来を表すID群を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表すID群の一部または全部を得る工程と、前記出所由来を表すID群が得られたときに、両プログラム実行・通信装置が、得られた出所由来を表すID群と自プログラム実行・通信装置内

のプロセスの元となる前記プログラムの出所由来を表すID群とを比較し、一致する前記プログラムの出所由来を表すIDが1つ以上存在すれば通信路を開く工程とを含むことを特徴とする。

【0048】また、本発明のプログラムID通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラムが、プログラム本体、該プログラムの出所由来を表す公開鍵、および該公開鍵と対をなす秘密鍵を含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置から相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵をそれぞれ得る工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程と、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致し、かつ相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証されたときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とする。

【0049】また、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵および秘密鍵を用いて相手プログラム実行・通信装置内のプロセスの元となるプログラムの相互認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、両プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵を相手プログラム実行・通信装置に送り、相手プログラム実行・通信装置にランダムな文字列をそれぞれ送り、相手プログラム実行・通信装置が、該文字列を相手プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した文字列を自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置が、暗号化された文字列に対応する公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置通信装置内のプロセスの元となるプログラ

ムを認証することを特徴とする。

【0050】さらに、本発明のプログラムID通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、前記プログラム本体に対し該公開鍵と対をなす秘密鍵により行った署名とを含み、あるプログラムを元にあるプログラム実行・通信装置が生成したあるプロセスが、該プログラムまたは別のあるプログラムを元に別のあるプログラム実行・通信装置が生成した別のあるプロセスと通信を行う前に、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程と、前記通信を行う前に、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであることが確認できた場合に、前記通信を行う前に、前記公開鍵を相手プログラム実行・通信装置に伝える工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致するかどうかを判定する工程と、相手プログラム実行・通信装置内のプロセスの元となるプログラムが相互認証され、かつ相手プログラム実行・通信装置から得られた公開鍵と自プログラム実行・通信装置内のプロセスの元となる前記プログラムの出所由来を表す公開鍵とが一致したときに、両プログラム実行・通信装置が通信路を開く工程とを含むことを特徴とする。

【0051】さらにまた、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、前記署名が前記プログラム本体と前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵とによって生成されたものであるかどうかを確認する工程において、前記署名が前記プログラム本体をハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す公開鍵と対をなす秘密鍵で暗号化した署名値からなり、両プログラム実行・通信装置が、前記署名値を前記プログラムの出所由来を表す公開鍵で復号してダイジェストを得るとともに前記プログラム本体をハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが一致するかどうかを判定することを特徴とする。

うかを判定することを特徴とする。

【0052】また、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の1つ以上の公開鍵とが一致するかどうかを判定することを特徴とする。

【0053】さらに、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする。

【0054】さらにまた、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の1つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする。

【0055】また、本発明のプログラムID通信範囲制御方法は、プログラムと、各プログラムを元に各プロセスを生成し実行する複数のプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、自プログラム実行・通信装置に付随する公開鍵および秘密鍵と、相手プログラム実行・通信装置に付随する公開鍵と、各プログラムを元に生成および実行されるプロセスとを含み、各プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵

群と、前記プログラム本体および前記公開鍵群を組み合わせ作成されたデータに対し各公開鍵と対をなす各秘密鍵により行った署名群とを含み、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせ作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを確認する工程と、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程と、両プログラム実行・通信装置が、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりを相手プログラム実行・通信装置に伝え、自プログラム実行・通信装置による署名確認結果の公開鍵の集まりと相手プログラム実行・通信装置による署名確認結果の公開鍵の集まりとに一致する公開鍵があるかどうかを判定する工程と、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵が1つ以上あるときに、両プログラム実行・通信装置が、プロセス間の通信路を開く工程とを含むことを特徴とする。

【0056】さらに、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、各署名が前記プログラム本体および前記公開鍵群を組み合わせ作成されたデータと各署名に対応する各公開鍵と対をなす各秘密鍵とによって生成されたものであるかどうかを判定する工程において、各署名が前記プログラム本体および前記公開鍵群を組み合わせ作成されたデータをハッシュ関数でハッシングしたダイジェストを前記プログラムの出所由来を表す各公開鍵と対をなす各秘密鍵で暗号化した各署名値からなり、相手プログラム実行・通信装置が、各署名値を前記プログラムの出所由来を表す各公開鍵でそれぞれ復号してダイジェスト群を得るとともに前記プログラム本体および前記公開鍵群で作成されたデータをハッシュ関数でハッシングしてダイジェストを得、該ダイジェストと前記ダイジェスト群とが一致するかどうかを判定することを特徴とする。

【0057】さらにまた、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の認証を行う工程において、両プログラム実行・通信装置が、通信してよい相手を示す公開鍵を備え、該通信してよい相手を示す公開鍵と相手プログラム実行・通信装置に付随する公開鍵群の1つ以上の公開鍵とが一致するかどうかを判定することを特徴とする。

【0058】また、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置に付随する公開鍵および秘密鍵を用いた公開鍵方式により相手プログラム実行・通信装置の

認証を行う工程において、公開鍵によるワン・タイム・パスワード方式が用いられ、自プログラム実行・通信装置は、相手プログラム実行・通信装置から相手プログラム実行・通信装置に付随する公開鍵を得、相手プログラム実行・通信装置にランダムな文字列を送り、相手プログラム実行・通信装置は、該文字列を相手プログラム実行・通信装置に付随する秘密鍵で暗号化して自プログラム実行・通信装置に送り返し、自プログラム実行・通信装置は、暗号化された文字列を相手プログラム実行・通信装置から得た前記公開鍵で復号し、復号した文字列と先に送った文字列とが一致すれば、相手プログラム実行・通信装置を認証することを特徴とする。

【0059】さらに、本発明のプログラムID通信範囲制御方法は、両プログラム実行・通信装置が、相手プログラム実行・通信装置の認証に成功し、かつ両プログラム実行・通信装置による署名確認結果の公開鍵の集まりに一致する公開鍵があるときに、プロセス間の通信路を開く工程において、両プログラム実行・通信装置が、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に存在する仮想通信路用資源群と、通信路用資源群とを含み、前記プログラムの出所由来を表す公開鍵が1つ以上得られた場合に、前記プログラムを元に生成されたプロセスが通信を行う際に、両プログラム実行・通信装置の通信装置が、得られた出所由来を表す公開鍵に対応する仮想通信路資源群の1つに通信路資源を割り当て、仮想通信路資源を使い通信路を提供することを特徴とする。

【0060】さらにまた、本発明のプログラムID通信範囲制御方法は、仮想通信路用資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路用資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする。

【0061】一方、本発明の公開鍵毎通信路提供方法は、プログラムと、該プログラムを元にプロセスを生成し実行および通信するプログラム実行・通信装置とにより構成される情報システムにおいて、前記プログラム実行・通信装置が、前記プログラムを元に生成および実行されるプロセスとを含み、前記プログラムが、プログラム本体と、該プログラムの出所由来を表す公開鍵と、通信路1つあたりに仮想的に複数の仮想通信路を形成する通信装置と、前記プログラムの出所由来を表す公開鍵毎に1つ以上存在する仮想通信路用資源と、1つ以上の通信路用資源とを含み、前記プログラム実行・通信装置が前記プログラムを元に生成されたプロセスの処理により通信を行う際に、出所由来を表す公開鍵と要求された仮想通信路用資源とを対にして仮想通信路と対応させ、仮想通信路を使い通信路を提供する工程を含むことを特

徴とする。

【0062】さらにまた、本発明の公開鍵毎通信路提供方法は、仮想通信路資源群が仮想的に定義したソケットであり、該仮想通信路資源群の一つ一つが該仮想的に定義したソケットの各ポートに対応し、通信路資源群が通常のソケットであり、各通信路資源群の一つ一つが該通常のソケット各ポートに対応することを特徴とする。

【0063】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0064】(1) 第1の実施の形態

図1を参照すると、本発明の第1の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器11と、通信機能を有する通信・処理装置が適用された親機器12と、携帯機器11にインストールされて実行されるプログラム112とから、その主要部が構成されている。

【0065】実行機能および通信機能は、Java (サンマイクロシステムズ社の登録商標) などが想定される。

【0066】携帯機器11としては、携帯電話機 (PHS (Personal HandyPhone) を含む)、携帯情報端末等が想定される。

【0067】親機器12としては、POS (Point Of Sales) 端末等が想定される。

【0068】携帯機器11と親機器12との間の通信機能は、エリクソン社等が提唱するBluetooth、無線LAN (Local Area Network)、PIAFS (PHS Internet Access Forum Standard) 等の近距離無線通信技術で実現されるものとする。

【0069】携帯機器11は、信頼できる組み込み機能部111と、プログラム112を実行するプロセス1120と、携帯機器11に付随する秘密鍵1131および公開鍵1132とを含んで構成されている。

【0070】プログラム112は、プログラム本体1121と、プログラム112の出所由来を表す公開鍵11221と、プログラム本体1121をハッシュ関数でハッシングしたダイジェストを公開鍵11221と対をなす秘密鍵 (図示せず) で暗号化した署名 (デジタル署名、電子署名) であるハッシュ値11231とを含んで構成されている。なお、プログラム112は、その出所 (製造元等) および由来 (バージョン等) において、プログラム本体1121、公開鍵11221、およびハッシュ値11231が一体として作成されている。

【0071】親機器12は、通信してよい相手を示す公開鍵として、携帯機器11に付随する公開鍵1132をもつ。

【0072】図2を参照すると、携帯機器11の組み込み機能部111および親機器12の処理は、ハッシュ値確認ステップS101と、通信要求発生ステップS102と、携帯機器認証ステップS103と、プログラム出所由来判定ステップS104と、プログラム認証ステップS105と、プログラム不認証ステップS106とからなる。

【0073】次に、このように構成された第1の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの動作について、図1および図2を参照して詳細に説明する。

【0074】まず、携帯機器11は、組み込み機能部111により、ハッシュ値11231がプログラム本体1121および公開鍵11221と対をなす秘密鍵とによって生成されたものであるかどうかを確認する (ステップS101)。詳しくは、組み込み機能部111は、ハッシュ値11231を公開鍵11221で復号してプログラム本体1121をハッシングしたダイジェストを得る一方、プログラム本体1121を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値11231がプログラム本体1121および公開鍵11221と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体1121および公開鍵11221が改竄されたものでなく、プログラム112が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器11にプログラム112が導入、たとえばダウンロードされたときに1回行われればよい。

【0075】次に、携帯機器11内のプログラム112を実行するプロセス1120が親機器12と通信をしようとして通信要求を発生させた場合 (ステップS102)、またはそれ以前に、親機器12は、携帯機器11に付随する公開鍵1132および秘密鍵1131を用いた公開鍵方式により携帯機器11の認証を行う (ステップS103)。

【0076】たとえば、親機器12は、自らが通信してよい相手を示す公開鍵として保持する携帯機器11に付随する公開鍵1132と、携帯機器11が保持する携帯機器11に付随する公開鍵1132とが一致するかどうかを判定し、一致した場合に携帯機器11の認証をおこなう。

【0077】また、RSA (Rivest, Shamir, Adleman) の公開鍵によるワン・タイム・パスワード (One Time Password) 方式を用いた場合、親機器12は携帯機器11にランダムな文字列を送り ("Challenge")、携帯機器11の組み込み機能部111はその文字列を携帯機器11に付随する秘密鍵1131で暗号化して親機器12に送り返し ("Response")、親機器12は暗号化

した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器 11 に付随する公開鍵 1132 で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器 11 を通信してよい相手（つまり、通信してよい相手を示す公開鍵として保持する携帯機器 11 に付随する公開鍵 1132 と対をなす秘密鍵 1131 を所有するもの）であると認証する。

【0078】携帯機器 11 の認証に成功した場合、親機器 12 は、携帯機器 11 の組み込み機能部 111 から携帯機器 11 によるハッシュ値確認結果の公開鍵 1122 10 1 を得、携帯機器 11 によるハッシュ値確認結果に基づいてプログラム 112 が真正な出所由来をもつものであるかどうかを判定し（ステップ S104）、そうであれば得られた公開鍵 11221 でプログラム 112 を認証したとする（ステップ S105）。

【0079】一方、携帯機器 11 の認証に失敗した場合（ステップ S103）、または公開鍵 11221 がプログラム 112 の真正な出所由来を表す公開鍵でなかった場合（ステップ S104）、親機器 12 は、プログラム 112 を認証しない。

【0080】第 1 の実施の形態によれば、プログラム 112 が秘密鍵をもたなくても、親機器 12 は、親機器 12 と通信をしようとしてきた携帯機器 11 内のプロセス 1120 の元となるプログラム 112 の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム 112 を元にして動作する携帯機器 11 と通信を行う場合に、親機器 12 がプログラム 112 の成りすましを防止しかつ認証を行うことができる。

【0081】（2） 第 2 の実施の形態

図 3 を参照すると、本発明の第 2 の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器 21 と、通信機能を有する通信・処理装置が適用された親機器 22 と、携帯機器 21 にインストールされて実行されるプログラム 212 20 2 から、その主要部が構成されている。

【0082】実行機能および通信機能は、Java など が想定される。

【0083】携帯機器 21 としては、携帯電話機（PHS を含む）、携帯情報端末等が想定される。

【0084】親機器 22 としては、POS 端末等が想定される。

【0085】携帯機器 21 と親機器 22 との間の通信機能は、エリクソン社等が提唱する Bluetooth、無線 LAN、PIAFS 等の近距離無線通信技術で実現されるものとする。

【0086】携帯機器 21 は、信頼できる組み込み機能部 211 と、プログラム 212 を実行するプロセス 2120 と、携帯機器 21 に付随する秘密鍵 2131 および公開鍵 2132 とを含んで構成されている。

【0087】プログラム 212 は、プログラム本体 2121 と、プログラム 212 の出所由来を表す公開鍵群 21221 ~ 2122n（n は 2 以上の正整数。以下同様）と、プログラム本体 2121 および公開鍵群 21221 ~ 2122n を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵 21221 ~ 2122n と対をなす各秘密鍵（図示せず）でそれぞれ暗号化した署名群であるハッシュ値群 21231 ~ 2123n とを含んで構成されている。なお、プログラム 212 は、その出所（製造元等）および由来（バージョン等）において、プログラム本体 2121、公開鍵群 21221 ~ 2122n、およびハッシュ値群 21231 ~ 2123n が一体として作成されている。

【0088】親機器 22 は、通信してよい相手を示す公開鍵として、携帯機器 21 に付随する公開鍵 2132 をもつ。

【0089】図 4 を参照すると、携帯機器 21 の組み込み機能部 211 および親機器 22 の処理は、ハッシュ値確認ステップ S201 と、通信要求発生ステップ S202 と、携帯機器認証ステップ S203 と、プログラム由来判定ステップ S204 と、プログラム認証ステップ S205 と、プログラム不認証ステップ S206 とからなる。

【0090】次に、このように構成された第 2 の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの動作について、図 3 および図 4 を参照して詳細に説明する。

【0091】まず、携帯機器 21 は、組み込み機能部 211 により、各ハッシュ値 21231 ~ 2123n がプログラム本体 2121 および公開鍵群 21221 ~ 2122n と各公開鍵 21221 ~ 2122n と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップ S201）。詳しくは、組み込み機能部 211 は、各ハッシュ値 21231 ~ 2123n を各公開鍵 21221 ~ 2122n でそれぞれ復号してプログラム本体 2221 および公開鍵群 21221 ~ 2122n を組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体 2121 および公開鍵群 21221 ~ 2122n を組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つとが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値 21231 ~ 2123n がプログラム本体 2121 および公開鍵群 21221 ~ 2122n と各公開鍵 21221 ~ 2122n と対をなす各秘密鍵とによって生成されたものであるかどうかをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体 2121 および公開鍵群 21221 ~ 2122n が、改竄されたものでなく、

プログラム 212 が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器 21 にプログラム 212 が導入、たとえばダウンロードされたときに 1 回行われればよい。

【0092】次に、携帯機器 21 内のプログラム 212 を実行するプロセス 2120 が親機器 22 と通信をしようとして通信要求が発生した場合(ステップ S202)、またはそれ以前に、親機器 22 は、携帯機器 21 に付随する秘密鍵 2131 および公開鍵 2132 を用いた公開鍵方式により携帯機器 21 の認証を行う (ステップ S203)。

【0093】たとえば、親機器 22 は、自らが通信してよい相手を示す公開鍵として保持する携帯機器 21 に付随する公開鍵 2132 と、携帯機器 21 が保持する携帯機器 21 に付随する公開鍵 2132 とが一致するかどうかを判定し、一致した場合に携帯機器 21 の認証を行う。

【0094】また、RSA の公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器 22 は携帯機器 21 にランダムな文字列を送り ("Challenge")、携帯機器 21 の組み込み機能部 211 はその文字列を携帯機器 21 に付随する秘密鍵 2131 で暗号化して親機器 22 に送り返し ("Response")、親機器 22 は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器 21 に付随する公開鍵 2132 で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器 21 を通信してよい相手 (つまり、通信してよい相手を示す公開鍵として保持する携帯機器 21 に付随する公開鍵 2132 と対をなす秘密鍵 2131 を所有するもの) であると認証する。

【0095】携帯機器 21 の認証に成功した場合、親機器 22 は、携帯機器 21 の組み込み機能部 211 から携帯機器 21 によるハッシュ値確認結果の公開鍵の集まりを得、携帯機器 21 によるハッシュ値確認結果の公開鍵の集まりに 1 つ以上の公開鍵が含まれていればプログラム 212 が真正な出所由来をもつものであると判定し (ステップ S204)、公開鍵の集まりの一部または全部でプログラム 212 を認証したとする (ステップ S205)。

【0096】一方、携帯機器 21 の認証に失敗した場合 (ステップ S203)、またはプログラム 212 の真正な出所由来を表す公開鍵が得られなかった場合 (ステップ S204)、親機器 22 は、プログラム 212 を認証しない (ステップ S206)。

【0097】なお、上記第 2 の実施の形態では、ステップ S204 で携帯機器 21 によるハッシュ値確認結果の公開鍵の集まりに 1 つ以上の公開鍵が含まれていればプログラム 212 が真正な出所由来をもつものであると判定したが、携帯機器 21 によるハッシュ値確認結果の公

開鍵の集まりに公開鍵群 21221 ~ 2122n のすべてが含まれていたときにのみプログラム 212 が真正な出所由来をもつものであると判定するようにすることもできる。

【0098】第 2 の実施の形態によれば、プログラム 212 が公開鍵群 21221 ~ 2122n をもつことを許す場合は、プログラム本体 2121 とともに保持する公開鍵群 21221 ~ 2122n に対し署名群であるハッシュ値群 21231 ~ 2123n を付与することから、プログラムの成りすましを防止することができる。

【0099】(2) 第 3 の実施の形態
図 5 を参照すると、本発明の第 3 の実施の形態に係るプログラム ID 通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器 31 と、通信機能を有する通信・処理装置が適用された親機器 32 と、携帯機器 31 にインストールされて実行されるプログラム 312 とから、その主要部が構成されている。

【0100】実行機能および通信機能は、Java など が想定される。

【0101】携帯機器 31 としては、携帯電話機 (PHS を含む)、携帯情報端末等が想定される。

【0102】親機器 32 としては、POS 端末等が想定される。

【0103】携帯機器 31 と親機器 32 との間の通信機能は、エリクソン社等が提唱する Bluetooth、無線 LAN、PIAFS 等の近距離無線通信技術で実現されるものとする。

【0104】携帯機器 31 は、信頼できる組み込み機能部 311 と、プログラム 312 を実行するプロセス 3120 とを含んで構成されている。

【0105】プログラム 312 は、プログラム本体 3121 と、プログラム 312 の出所由来を表す公開鍵 31221 および秘密鍵 31241 とを含んで構成されている。なお、プログラム 312 は、その出所 (製造元等) および由来 (バージョン等) において、プログラム本体 3121、公開鍵 31221、および秘密鍵 31241 が一体として作成されている。

【0106】図 6 を参照すると、携帯機器 31 の組み込み機能部 311 および親機器 32 の処理は、通信要求発生ステップ S301 と、公開鍵獲得ステップ S302 と、プログラム認証ステップ S303 と、通信・処理ステップ S304 と、通信・処理なしステップ S305 とからなる。

【0107】次に、このように構成された第 3 の実施の形態に係るプログラム ID 通信処理制御方法が適用された情報システムの動作について、図 5 および図 6 を参照して詳細に説明する。

【0108】携帯機器 31 内のプログラム 312 を実行するプロセス 3120 が親機器 32 と通信するための通

信要求を発生させた場合（ステップS301）、親機器32は、携帯機器31の組み込み機能部311を介して、プロセス3120の元となるプログラム312の出所由来を表す公開鍵31221を得る（ステップS302）。

【0109】次に、親機器32は、携帯機器31の組み込み機能部311に対し、公開鍵31221および秘密鍵31241を用いた公開鍵方式によりプロセス3120の元となるプログラム312が真正な出所由来をもつものであるかどうかを認証する（ステップS303）。 10

【0110】たとえば、RSAの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器32は携帯機器31の組み込み部311にランダムな文字列を送り（“Challenge”）、携帯機器31の組み込み機能部311はその文字列をプロセス3120の元となるプログラム312の出所由来を表す公開鍵31221と対をなす秘密鍵31241で暗号化して親機器32に送り返し（“Response”）、親機器32は暗号化した文字列を先に受け取った公開鍵31221で復号し、復号した文字列と先に送ったランダムな文字列とが 20 一致すれば、プロセス3120の元となるプログラム312は真正な出所由来をもつものである（つまり、プログラム312が該プログラム312の出所由来を表す公開鍵31221と対をなす秘密鍵31241を所有する）と認証する。

【0111】プログラム312の認証に成功した場合（ステップS303）、親機器32は、以降の通信によって発生する処理を、公開鍵31221に対応するユーザ権限でアクセス制御して実行する（ステップS304）。 30

【0112】一方、プログラム312の認証に失敗した場合（ステップS303）、または公開鍵31221に対応するユーザ権限が存在しない場合、親機器32は、通信によって発生する処理をしないか、特定の制限されたユーザ権限で処理を実行する（ステップS305）。

【0113】第3の実施の形態によれば、プログラム312の出所由来を表す公開鍵31221、つまりプログラム312の製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うことから、悪意のプログラムに対しセキュリティを保つことができる。

【0114】また、プログラム312の出所由来を表す公開鍵31221、つまりプログラム312の製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うため、ユーザ管理のような集中管理が困難な分散環境下での通信による処理について、悪意のプログラムに対しセキュリティを保つことができる。

【0115】（4） 第4の実施の形態

図7を参照すると、本発明の第4の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行 50

・通信装置が適用された携帯機器41と、通信機能を有する通信・処理装置が適用された親機器42と、携帯機器41にインストールされ実行されるプログラム412とから、その主要部が構成されている。

【0116】実行機能および通信機能は、Javaなどが想定される。

【0117】携帯機器41としては、携帯電話機（PHSを含む）、携帯情報端末等が想定される。

【0118】親機器42としては、POS端末等が想定される。

【0119】携帯機器41と親機器42との間の通信機能は、エリクソン社等が提唱するBluetooth、無線LAN、PIAFS等の近距離無線通信技術で実現されるものとする。

【0120】携帯機器41は、信頼できる組み込み機能部411と、プログラム412を実行するプロセス4120と、携帯機器41に付随する秘密鍵4131および公開鍵4132とを含んで構成されている。

【0121】プログラム412は、プログラム本体4121と、プログラム412の出所由来を表す公開鍵41221と、プログラム本体4121をハッシュ関数でハッシングしたダイジェストを公開鍵41221と対をなす秘密鍵（図示せず）で暗号化した署名であるハッシュ値41231とを含んで構成されている。なお、プログラム412は、その出所（製造元等）および由来（バージョン等）において、プログラム本体4121、公開鍵41221、およびハッシュ値41231が一体として作成されている。

【0122】親機器42は、通信してよい相手を示す公開鍵として、携帯機器41に付随する公開鍵4132をもつ。

【0123】図8を参照すると、携帯機器41の組み込み機能部411および親機器42の処理は、ハッシュ値確認ステップS401と、通信要求発生ステップS402と、携帯機器認証ステップS403と、プログラム出所由来判定ステップS404と、通信・処理ステップS405と、通信・処理なしステップS406とからなる。

【0124】次に、このように構成された第4の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの動作について、図7および図8を参照して詳細に説明する。

【0125】まず、携帯機器41は、組み込み機能部411により、ハッシュ値41231がプログラム本体4121および公開鍵41221と対をなす秘密鍵とによって生成されたものであるかどうかを確認する（ステップS401）。詳しくは、組み込み機能部411は、ハッシュ値41231を公開鍵41221で復号してプログラム本体4121をハッシングしたダイジェストを得る一方、プログラム本体4121を既知のハッシュ関数

でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値41231がプログラム本体4121および公開鍵41221と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体4121および公開鍵41221が改竄されたものでなく、プログラム412が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器41にプログラム412が導入、たとえばダウンロードされたときに1行われればよい。

【0126】次に、携帯機器41内のプログラム412を実行するプロセス4120が親機器42と通信をしようとして通信要求を発生させた場合(ステップS402)、またはそれ以前に、親機器42は、携帯機器41に付随する公開鍵4132および秘密鍵4131を用いた公開鍵方式により携帯機器41の認証を行う(ステップS403)。

【0127】たとえば、親機器42は、自らが通信してよい相手を示す公開鍵として保持する携帯機器41に付随する公開鍵4132と、携帯機器41が保持する携帯機器41に付随する公開鍵4132とが一致するかどうかを判定し、一致した場合に携帯機器41を認証する。

【0128】また、RSAの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器42は携帯機器41にランダムな文字列を送り(“Challenge”)、携帯機器41の組み込み機能部411はその文字列を携帯機器41に付随する秘密鍵4131で暗号化して親機器42に送り返し(“Response”)、親機器42は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器41に付随する公開鍵4132で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器41を通信してよい相手(つまり、通信してよい相手を示す公開鍵として保持する携帯機器41に付随する公開鍵4132と対をなす秘密鍵4131を所有するもの)であると認証する。

【0129】携帯機器41の認証に成功した場合、親機器42は、携帯機器41の組み込み機能部411から公開鍵41221を得、携帯機器41によるハッシュ値確認結果に基づいてプログラム412が真正な出所由来をもつものであるかどうかを判定し(ステップS404)、そうであれば以降の通信によって発生する処理を公開鍵41221に対応するユーザ権限でアクセス制御して実行する(ステップS405)。

【0130】一方、携帯機器41の認証に失敗した場合(ステップS403)、プログラム412が真正な出所由来をもつものでなかった場合(ステップS404)、または公開鍵41221に対応するユーザ権限が存在しない場合、親機器42は、通信によって発生する処理を実行しないか、特定の決められたユーザ権限でアクセス

制御して実行する(ステップS406)。

【0131】第4の実施の形態によれば、プログラム412が秘密鍵をもたなくても、親機器42は、親機器42と通信をしようとしてきた携帯機器41内のプロセス4120の元となるプログラム412の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム412を元にして動作する携帯機器41と通信を行う場合に、親機器42がプログラム412の成りすましを防止しかつ認証を行うことができる。

10 【0132】(5) 第5の実施の形態

図9を参照すると、本発明の第5の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムは、実行機能および通信機能を有するプログラム実行・通信装置が適用された携帯機器51と、通信機能を有する通信・処理装置が適用された親機器52と、携帯機器51にインストールされ実行されるプログラム512とから、その主要部が構成されている。

【0133】実行機能および通信機能は、Javaなどが想定される。

20 【0134】携帯機器51としては、携帯電話機(PHSを含む)、携帯情報端末等が想定される。

【0135】親機器52としては、POS端末等が想定される。

【0136】携帯機器51と親機器52との間の通信機能は、エリクソン社等が提唱するBluetooth、無線LAN、PIAFS等の近距離無線通信技術で実現されるものとする。

30 【0137】携帯機器51は、信頼できる組み込み機能部511と、プログラム512を実行するプロセス5120と、携帯機器51に付随する秘密鍵5131および公開鍵5132とを含んで構成されている。

【0138】プログラム512は、プログラム本体5121と、プログラム512の出所由来を表す公開鍵群51221~5122nと、プログラム本体5121および公開鍵群51221~5122nを組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵51221~5122nと対をなす各秘密鍵(図示せず)でそれぞれ暗号化した署名群であるハッシュ値群51231~5123nとを含んで構成されている。なお、プログラム512は、その出所(製造元等)および由来(バージョン等)において、プログラム本体5121、公開鍵群51221~5122n、およびハッシュ値群51231~5123nが一体として作成されている。

【0139】親機器52は、通信してよい相手を示す公開鍵として、携帯機器51に付随する公開鍵5132をもつ。

【0140】図10を参照すると、携帯機器51の組み込み機能部511および親機器52の処理は、ハッシュ値確認ステップS501と、通信要求発生ステップS5

02と、携帯機器認証ステップS503と、プログラム出所由来判定ステップS504と、通信・処理ステップS505と、通信・処理なしステップS506とからなる。

【0141】次に、このように構成された第5の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの動作について、図9および図10を参照して詳細に説明する。

【0142】まず、携帯機器51は、組み込み機能部511により、各ハッシュ値51231～5123nがプログラム本体5121および公開鍵群51221～5122nと各公開鍵51221～5122nと対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る(ステップS501)。詳しくは、組み込み機能部511は、各ハッシュ値51231～5123nを各公開鍵51221～5122nでそれぞれ復号してプログラム本体5121および公開鍵群51221～5122nを組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体5121および公開鍵群51221～5122nを組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つとが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値51231～5123nがプログラム本体5121および公開鍵群51221～5122nと各公開鍵51221～5122nと対をなす各秘密鍵とによって生成されたものであるかどうかをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体5121および公開鍵群51221～5122nが、改竄されたものでなく、プログラム512が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器51にプログラム512が導入、たとえばダウンロードされたときに1回行われればよい。

【0143】次に、携帯機器51内のプログラム512を実行するプロセス5120が親機器52と通信をしようとして通信要求が発生した場合(ステップS502)、またはそれ以前に、親機器52は、携帯機器51に付随する公開鍵5132および秘密鍵5131を用いた公開鍵方式により携帯機器51の認証を行う(ステップS503)。

【0144】たとえば、親機器52は、自らが通信してよい相手を示す公開鍵として保持する携帯機器51に付随する公開鍵5132と、携帯機器51が保持する携帯機器51に付随する公開鍵5132とが一致するかどうかを判定し、一致した場合に携帯機器51の認証を行う。

【0145】また、RSAの公開鍵によるワン・タイム・パスワード方式を用いた場合、親機器52は携帯機器

51にランダムな文字列を送り(“Challenge”)、携帯機器51の組み込み機能部511はその文字列を携帯機器51に付随する秘密鍵5131で暗号化して親機器52に送り返し(“Response”)、親機器52は暗号化した文字列を事前に通信してよい相手を示す公開鍵として保持する携帯機器51に付随する公開鍵5132で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器51を通信してよい相手(つまり、通信してよい相手を示す公開鍵として保持する携帯機器51に付随する公開鍵5132と対をなす秘密鍵5131を所有するもの)であると認証する。

【0146】携帯機器51の認証に成功した場合、親機器52は、携帯機器51の組み込み機能部511からハッシュ値確認結果の公開鍵の集まりを得、携帯機器51によるハッシュ値確認結果の公開鍵の集まりに1つ以上の公開鍵が含まれていればプログラム512が真正な出所由来をもつものであると判定し(ステップS504)、以降の通信によって発生する処理をハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行する(ステップS505)。

【0147】一方、携帯機器51の認証に失敗した場合(ステップS503)、プログラム512が真正な出所由来をもつものでない場合(ステップS504)、または携帯機器51によるハッシュ値確認結果の公開鍵の集まり中の公開鍵に対応するユーザ権限が1つも存在しない場合、親機器52は、通信によって発生する処理を実行しないか、特定の制限されたユーザ権限でアクセス制御して実行する(ステップS506)。

【0148】なお、上記第5の実施の形態では、ステップS504で携帯機器51によるハッシュ値確認結果の公開鍵の集まりに1つ以上の公開鍵が含まれていればプログラム512が真正な出所由来をもつものであると判定したが、携帯機器51によるハッシュ値確認結果の公開鍵の集まりに公開鍵群51221～5122nのすべてが含まれていたときにのみプログラム512が真正な出所由来をもつものであると判定するようにすることもできる。

【0149】第5の実施の形態によれば、プログラム512が該プログラム512の出所由来を表す公開鍵群51221～5122nをもつことを許す場合はプログラム本体5121とともに保持する公開鍵群51221～5122nに対して署名群であるハッシュ値群51231～5123nを付すことから、プログラム512の成りすましを防止することができ、通信によって発生する処理をハッシュ値確認結果の公開鍵の集まりの各公開鍵に対応するユーザ権限の組み合わせでアクセス制御して実行することができる。

【0150】(6) 第6の実施の形態

図 11 を参照すると、本発明の第 6 の実施の形態に係るプログラム ID 通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器 61 と、同じくプログラムの実行機能および通信機能を有する親機器 62 と、携帯機器 61 にインストールされ実行されるプログラム 612 と、親機器 62 にインストールされ実行されるプログラム 622 とから、その主要部が構成されている。

【0151】実行機能および通信機能は、Java など
10 が想定される。

【0152】携帯機器 61 としては、携帯電話機 (PHS を含む)、携帯情報端末等が想定される。

【0153】親機器 62 としては、POS 端末等が想定される。

【0154】携帯機器 61 と親機器 62 との間の通信機能に使用される通信方式は、エリクソン社等が提唱する Bluetooth、無線 LAN、PIAFS 等の近距離無線通信技術で実現されるものとする。

【0155】携帯機器 61 は、信頼できる組み込み機能部 611 と、プログラム 612 を実行するプロセス 61
20 20 とを含んで構成されている。

【0156】プログラム 612 は、プログラム本体 6121 と、プログラム 612 の出所由来を表す公開鍵 6122 および秘密鍵 6124 とを含んで構成されている。なお、プログラム 612 は、その出所 (製造元等) および由来 (バージョン等) において、プログラム本体 6121、公開鍵 6122 および秘密鍵 6124 が一体として作成されている。

【0157】親機器 62 は、信頼できる組み込み機能部 621 と、プログラム 622 を実行するプロセス 62
30 20 とを含んで構成されている。

【0158】プログラム 622 は、プログラム本体 6221 と、プログラム 622 の出所由来を表す公開鍵 6222 および秘密鍵 6224 とを含んで構成されている。なお、プログラム 622 は、その出所 (製造元等) および由来 (バージョン等) において、プログラム本体 6221、公開鍵 6222 および秘密鍵 6224 が一体として作成されている。

【0159】図 12 を参照すると、携帯機器 61 の組み込み機能部 611 および親機器 62 の組み込み機能部 6
40 21 の処理は、通信要求発生ステップ S601 と、公開鍵獲得ステップ S602 と、相互認証ステップ S603 と、公開鍵比較ステップ S604 と、相互認証・公開鍵一致判定ステップ S605 と、通信許可ステップ S606 と、通信不許可ステップ S607 とからなる。

【0160】次に、このように構成された第 6 の実施の形態に係るプログラム ID 通信範囲制御方法が適用された情報システムの動作について、図 11 および図 12 を参照して詳細に説明する。

【0161】携帯機器 61 内のプログラム 612 を実行 50

するプロセス 6120 と親機器 62 内のプログラム 622 を実行するプロセス 6220 との間で通信要求が発生した場合 (ステップ S601)、まず、携帯機器 61 の組み込み機能部 611 は、親機器 62 の組み込み機能部 621 にプロセス 6120 の元となるプログラム 612 の出所由来を表す公開鍵 6122 を送り、親機器 62 の組み込み機能部 621 は、携帯機器 61 の組み込み機能部 611 にプロセス 6220 の元となるプログラム 622 の出所由来を表す公開鍵 6222 を送り (ステップ S
602)、次に、双方で、公開鍵 6122 と公開鍵 6222 とが一致するかどうかを調べる (ステップ S603)。

【0162】次に、携帯機器 61 の組み込み機能部 611 と親機器 62 の組み込み機能部 621 との間で、プログラム 612 およびプログラム 622 の相互認証を行う (ステップ S604)。

【0163】たとえば、RSA の公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器 61 の組み込み機能部 611 は親機器 62 の組み込み機能部 621 にランダムな文字列を送り ("Challenge")、親機器 62 の組み込み機能部 621 はその文字列をプログラム 622 の秘密鍵 6224 で暗号化して携帯機器 61 の組み込み機能部 611 に送り返し ("Response")、携帯機器 61 の組み込み機能部 611 は、暗号化した文字列を公開鍵 6222 で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス 6220 の元となるプログラム 622 が公開鍵 6222 をもつ (つまり、プロセス 6220 の元となるプログラム 622 が公開鍵 6222 と対をなす秘密鍵 6224 をもつ) と認証する。

【0164】一方、親機器 62 の組み込み機能部 621 は携帯機器 61 の組み込み機能部 611 にランダムな文字列を送り ("Challenge")、携帯機器 61 の組み込み機能部 611 はその文字列を携帯機器 61 に付随する秘密鍵 6124 で暗号化して親機器 62 の組み込み機能部 621 に送り返し ("Response")、親機器 62 の組み込み機能部 621 は、暗号化した文字列を公開鍵 6122 で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、プロセス 6120 の元となるプログラム 612 が公開鍵 6122 をもつ (つまり、プロセス 6120 の元となるプログラム 612 が公開鍵 6122 と対をなす秘密鍵 6124 をもつ) と認証する。

【0165】プログラム 611 およびプログラム 612 の相互認証が成功し、かつ公開鍵 6122 と公開鍵 6222 とが一致した場合 (ステップ S605)、携帯機器 61 の組み込み機能部 611 および親機器 62 の組み込み機能部 621 は、プロセス 61210 とプロセス 62210 との間で通信を許可する (ステップ S606)。

【0166】逆に、プログラム 611 およびプログラム

612の相互認証に失敗した場合、あるいはプログラム612の出所由来を表す公開鍵6122とプログラム622の出所由来を表す公開鍵6222とが一致しなかった場合、携帯機器61の組み込み機能部611および親機器62の組み込み機能部621は、プロセス6120とプロセス6220との間で通信を不許可とする(ステップS607)。

【0167】第6の実施の形態によれば、携帯機器61内のプログラム612および親機器62内のプログラム622が、一致する公開鍵6122および6222を付随するプログラム612および622としか通信できず、任意の他のプログラムと通信できないため、携帯機器61内のプログラム612および親機器62内のプログラム622のもつ情報の、流通する範囲を出所由来を同じくするプログラムの範囲内に限ることができる。

【0168】また、携帯機器61内のプログラム612および親機器62内のプログラム622が、一致する公開鍵6122および6222を付随するプログラム612および622としか通信できず、任意の他のプログラムと通信できないため、携帯機器61内のプログラム612および親機器62内のプログラム622のもつ情報が、たとえプログラム612および622が暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しない。

【0169】さらに、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の1つである通信時の情報漏洩について、製造元またはそれに類するものを同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ、暴走による漏洩が起こらず、また、逆に1つのサービスにおいては、そのプロジェクトにかかわるもの全体である1つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【0170】(7) 第7の実施の形態

図13を参照すると、本発明の第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器71と、同じくプログラムの実行機能および通信機能を有する親機器72と、携帯機器71にインストールされ実行されるプログラム712と、親機器72にインストールされ実行されるプログラム722とから、その主要部が構成されている。

【0171】実行機能および通信機能は、Javaなどが想定される。

【0172】携帯機器71としては、携帯電話機(PHSを含む)、携帯情報端末等が想定される。

【0173】親機器72としては、POS端末等が想定

される。

【0174】携帯機器71と親機器72との間の通信機能に使用される通信方式は、エリクソン社等が提唱するBluetooth、無線LAN、PIAFS等の近距離無線通信技術で実現されるものとする。

【0175】携帯機器71は、信頼できる組み込み機能部711と、プログラム712を実行するプロセス7120と、携帯機器71に付随する秘密鍵7131および公開鍵7132と、親機器72に付随する公開鍵7232とを含んで構成されている。

【0176】プログラム712は、プログラム本体7121と、プログラム712の出所由来を表す公開鍵7122と、プログラム本体7121をハッシュ関数でハッシュしたダイジェストを公開鍵7122と対をなす秘密鍵(図示せず)で暗号化した署名であるハッシュ値7123とを含んで構成されている。なお、プログラム712は、その出所(製造元等)および由来(バージョン等)においてプログラム本体7121、公開鍵7122、およびハッシュ値7123が一体として作成されている。

【0177】親機器72は、信頼できる組み込み機能部721と、プログラム722を実行するプロセス7220と、親機器72に付随する秘密鍵7231および公開鍵7232と、携帯機器71に付随する公開鍵7132とを含んで構成されている。

【0178】プログラム722は、プログラム本体7221と、プログラム722の出所由来を表す公開鍵7222と、プログラム本体7221をハッシュ関数でハッシュしたダイジェストを公開鍵7222と対をなす秘密鍵(図示せず)で暗号化した署名であるハッシュ値7223とを含んで構成されている。なお、プログラム722は、その出所(製造元等)および由来(バージョン等)において、プログラム本体7221、公開鍵7222、およびハッシュ値7223が一体として作成されている。

【0179】図14を参照すると、携帯機器71の組み込み機能部711および親機器72の組み込み機能部721の処理は、ハッシュ値確認ステップS701およびS702と、通信要求発生ステップS703と、相互認証ステップS704と、公開鍵一致判定ステップS705と、通信許可ステップS706と、通信不許可ステップS707とからなる。

【0180】次に、このように構成された第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの動作について、図13および図14を参照して詳細に説明する。

【0181】まず、携帯機器71は、組み込み機能部711により、ハッシュ値7123がプログラム本体7121および公開鍵群7122と公開鍵7122と対をなす秘密鍵とによって生成されたものであるかどうかを確

認する(ステップS701)。詳しくは、組み込み機能部711は、ハッシュ値7123を公開鍵7122で復号してプログラム本体7221をハッシングしたダイジェストを得る一方、プログラム本体7121を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値7123がプログラム本体7121および公開鍵群7122と公開鍵7122と対をなす秘密鍵とによって生成されたものであるかどうかを確認する。すなわち、プログラム本体7121および公開鍵7122が改竄されたものでなく、プログラム712が真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器71にプログラム712が導入、たとえばダウンロードされたときなどに1回行われればよい。

【0182】また、親機器72も、組み込み機能部721により、ハッシュ値7223がプログラム本体7221および公開鍵群7222と公開鍵7222と対をなす秘密鍵とによって生成されたものであるかどうかを確認する(ステップS702)。詳しくは、組み込み機能部721は、ハッシュ値7223を公開鍵7222で復号してプログラム本体7221をハッシングしたダイジェストを得る一方、プログラム本体7221を既知のハッシュ関数でハッシングしてダイジェストを得、両ダイジェストが完全に一致するかどうかを検証することで、ハッシュ値7223がプログラム本体7221および公開鍵群7222と公開鍵7222と対をなす秘密鍵とによって生成されたものであることを確認する。すなわち、プログラム本体7221および公開鍵7222が改竄されたものでなく、プログラム722が真正な出所由来をもつことを確認する。なお、この確認処理は、親機器72にプログラム722が導入、たとえばインストールされたときなどに1回行われればよい。

【0183】次に、携帯機器71内のプログラム712を実行するプロセス7120と親機器72内のプログラム722を実行するプロセス7220とが通信をしようとして通信要求が発生した場合(ステップS703)、またはそれ以前に、まず、携帯機器71の組み込み機能部711と親機器72の組み込み機能部721との間で、携帯機器71が付随する秘密鍵7131および公開鍵7132と、親機器72が付随する秘密鍵7231および公開鍵7232とを用いた公開鍵方式により携帯機器71および親機器72の相互認証を行う(ステップS704)。

【0184】たとえば、親機器72は、自らが通信してよい相手を示す公開鍵として保持する携帯機器71に付随する公開鍵7132と、携帯機器71が保持する携帯機器71に付随する公開鍵71132とが一致するかどうかを判定し、一致した場合に携帯機器71の認証を行う。一方、携帯機器71は、自らが通信してよい相手を示す公開鍵として保持する親機器72に付随する公開鍵

7232と、親機器72が保持する親機器72に付随する公開鍵72132とが一致するかどうかを判定し、一致した場合に親機器72の認証を行う。

【0185】また、RSAの公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器71の組み込み機能部711は親機器72にランダムな文字列を送り(“Challenge”)、親機器72の組み込み機能部721はその文字列を親機器72に付随する秘密鍵7231で暗号化して携帯機器71に送り返し(“Response”)、携帯機器71の組み込み機能部711は、暗号化した文字列を親機器72に付随する公開鍵7232で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、親機器72を通信してよい相手(つまり、親機器72に付随する公開鍵7232と対をなす秘密鍵7231を所有するもの)であると認証する。一方、親機器72の組み込み機能部721は携帯機器71にランダムな文字列を送り(“Challenge”)、携帯機器71の組み込み機能部711はその文字列を携帯機器71に付随する秘密鍵7131で暗号化して親機器72に送り返し(“Response”)、親機器72の組み込み機能部721は暗号化した文字列を携帯機器71に付随する公開鍵7132で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば携帯機器71を通信してよい相手(つまり、携帯機器71に付随する公開鍵7132と対をなす秘密鍵7131を所有するもの)であると認証する。

【0186】相互認証に成功した場合、携帯機器71の組み込み機能部711および親機器72の組み込み機能部721は、プログラム712の出所由来を表す公開鍵7122とプログラム722の出所由来を表す公開鍵7222とをお互いに相手に伝え、両公開鍵が一致するかどうかを判定し(ステップS705)、一致した場合に限り、プロセス71210とプロセス72210との間で通信を許可する(ステップS706)。

【0187】携帯機器71と親機器72との相互認証に失敗した場合(ステップS704)、またはプログラム712の出所由来を表す公開鍵7122とプログラム722の出所由来を表す公開鍵7222とが一致しなかった場合(ステップS705)、携帯機器71の組み込み機能部711および親機器72の組み込み機能部721は、プロセス7120とプロセス7220との間の通信を不許可とする(ステップS707)。

【0188】第7の実施の形態によれば、携帯機器71内のプログラム712および親機器72内のプログラム722が、一致する公開鍵7122および7222を付随するプログラム712および722としか通信できず、任意の他のプログラムと通信できないため、携帯機器71内のプログラム712および親機器72内のプログラム722のもつ情報の、流通する範囲を出所由来を同じくするプログラムの範囲内に限ることができる。

【0189】また、携帯機器71内のプログラム712および親機器72内のプログラム722が、一致する公開鍵7122および7222を付随するプログラム712および722としか通信できず、任意の他のプログラムと通信できないため、携帯機器71内のプログラム712および親機器72内のプログラム722のもつ情報が、たとえプログラム712および722が暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しない。

【0190】さらに、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の1つである通信時の情報漏洩について、製造元またはそれに類するものと同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ、暴走による漏洩が起こらず、また、逆に1つのサービスにおいては、そのプロジェクトにかかわるもの全体である1つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【0191】さらに、プログラム712、722が秘密鍵をもたなくても、携帯機器71および親機72は、相手内のプロセス7220、7120、の元となるプログラム722、712の認証が可能であることから、盗み見や改竄が可能な環境下にあるプログラム712、722を元にして動作する相手と通信を行う場合に、携帯機器71、親機器72がプログラム722、712の成りすましを防止しかつ認証を行うことができる。

【0192】(8) 第8の実施の形態

図15を参照すると、本発明の第8の実施の形態に係るプログラムID通信範囲制御方法および公開鍵毎通信路提供方法が適用された情報システムは、第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムにおいて、携帯機器81および親機器82が、さらに、通信装置815および825と、公開鍵毎にすべてのポート番号を割り振ることの出来る、つまり同じポート番号で公開鍵毎に存在し得る仮想ソケット81511~8151iおよび82611~8251jと、ソケット81521~8152kおよび82521~8252lとを含んで構成されている。なお、第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムにおける部分と対応する部分には、符号の先頭文字「7」を「8」に変更した符号を付して、それらの詳しい説明を省略する。

【0193】仮想ソケット81511~8151iおよび82611~8251jは、チャネル、パイプ等の他の通信路を仮想的にしたものでもよく、ソケット81521~8152kおよび82521~8252l、チャネル、パイプ等の他の通信路であってもよい。

【0194】図16を参照すると、携帯機器81の組み込み機能部811および親機器82の組み込み機能部821の処理は、ハッシュ値確認ステップS801およびS802と、通信要求発生ステップS803と、相互認証ステップS804と、公開鍵一致判定ステップS805と、通信許可ステップS806と、通信不許可ステップS807とからなる。

【0195】次に、このように構成された第8の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの動作について、図15および図16を参照して詳細に説明する。

【0196】ステップS801~ステップS805およびステップS807は、第7の実施の形態に係るプログラムID通信範囲制御方法におけるステップS701~ステップS705およびステップS707と同じである。

【0197】第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの動作において、プロセス8120とプロセス8220との間で通信を許可するステップS806において、一致した場合に限り、通信装置815および825は、それぞれ、公開鍵8122および8222とプロセス81210およびプロセス82210が要求する仮想ソケットのポート番号の対に対し、組み込み機能部811と組み込み機能部821との間で使用しているソケットによる通信路に形成された仮想通信路の1つを割り当て、該仮想通信路によりプロセス81210とプロセス82210との間での通信を許可する。

【0198】(9) 第9の実施の形態

図17を参照すると、本発明の第9の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムは、プログラムの実行機能および通信機能を有する携帯機器91と、同じくプログラムの実行機能および通信機能を有する親機器92と、携帯機器91にインストールされ実行されるプログラム912と、親機器92にインストールされ実行されるプログラム922とから、その主要部が構成されている。

【0199】実行機能および通信機能は、Javaなどが想定される。

【0200】携帯機器91としては、携帯電話機(PHSを含む)、携帯情報端末等が想定される。

【0201】親機器92としては、POS端末等が想定される。

【0202】携帯機器91と親機器92との間の通信機能に使用される通信方式は、エリクソン社等が提唱するBluetooth、無線LAN、PIAFS等の近距離無線通信技術で実現されるものとする。

【0203】携帯機器91は、信頼できる組み込み機能部911と、プログラム912を実行するプロセス9120と、携帯機器91に付随する秘密鍵9131および

公開鍵 9132 と、親機器 92 に付随する公開鍵 9232 とを含んで構成されている。

【0204】プログラム 912 は、プログラム本体 9121 と、プログラム 912 の出所由来を表す公開鍵群 91221 ~ 9122n と、プログラム本体 9121 および公開鍵群 91221 ~ 9122n を組み合わせて作成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵 91221 ~ 9122n と対をなす各秘密鍵（図示せず）で暗号化した署名群であるハッシュ値群 91231 ~ 9123n とを含んで構成されている。なお、プログラム 912 は、その出所（製造元等）および由来（バージョン等）において、プログラム本体 9121、公開鍵群 91221 ~ 9122n、およびハッシュ値群 91231 ~ 9123n が一体として作成されている。

【0205】親機器 92 は、信頼できる組み込み機能部 921 と、プログラム 922 を実行するプロセス 9220 と、親機器 92 に付随する秘密鍵 9231 および公開鍵 9232 と、携帯機器 91 に付随する公開鍵 9132 とを含んで構成されている。

【0206】プログラム 922 は、プログラム本体 9221 と、プログラム 922 の出所由来を表す公開鍵群 92221 ~ 9222m（m は 2 以上の正整数。以下同様）と、プログラム本体 9221 および公開鍵群 92221 ~ 9222m により構成されたデータをハッシュ関数でハッシングしたダイジェストを各公開鍵 92221 ~ 9222m と対をなす各秘密鍵（図示せず）で暗号化した署名群であるハッシュ値群 92231 ~ 9223m とを含んで構成されている。なお、プログラム 922 は、その出所（製造元等）および由来（バージョン等）において、プログラム本体 9221、公開鍵群 92221 ~ 9222m、およびハッシュ値群 92231 ~ 9223m が一体として作成されている。

【0207】図 18 を参照すると、携帯機器 91 の組み込み機能部 911 および親機器 92 の組み込み機能部 921 の処理は、ハッシュ値確認ステップ S901 および S902 と、通信要求発生ステップ S903 と、相互認証ステップ S904 と、公開鍵一致判定ステップ S905 と、通信許可ステップ S906 と、通信不許可ステップ S907 とからなる。

【0208】次に、このように構成された第 9 の実施の形態に係るプログラム ID 通信範囲制御方法が適用された情報システムの動作について、図 17 および図 18 を参照して詳細に説明する。

【0209】まず、携帯機器 91 は、組み込み機能部 911 により、各ハッシュ値 91231 ~ 9123n がプログラム本体 9121 および公開鍵群 91221 ~ 9122n と各公開鍵 91221 ~ 9122n と対をなす各秘密鍵とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得

る（ステップ S901）。詳しくは、組み込み機能部 911 は、各ハッシュ値 91231 ~ 9123n を各公開鍵 91221 ~ 9122n でそれぞれ復号してプログラム本体 9121 および公開鍵群 91221 ~ 9122n を組み合わせて作成されたデータをハッシングしたダイジェスト群を得る一方、プログラム本体 9121 および公開鍵群 91221 ~ 9122n を組み合わせて作成されたデータを既知のハッシュ関数でハッシングしてダイジェストを得、該ダイジェストとダイジェスト群の一つ一つが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値 91231 ~ 9123n がプログラム本体 9121 および公開鍵群 91221 ~ 9122n と各公開鍵 91221 ~ 9122n と対をなす各秘密鍵とによって生成されたものであることをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体 9121 および公開鍵群 91221 ~ 9122n 中の少なくとも 1 つ以上の公開鍵が改竄されたものでなく、真正な出所由来をもつことを確認する。なお、この確認処理は、携帯機器 91 にプログラム 912 が導入、たとえばダウンロードされたときなどに 1 回行われればよい。

【0210】また、携帯機器 92 でも、組み込み機能部 921 が、各ハッシュ値 92231 ~ 9223n がプログラム本体 9221 および公開鍵群 92221 ~ 9222n と各公開鍵 92221 ~ 9222n と対をなす各秘密鍵（図示せず）とによって生成されたものであるかどうかを確認し、確認したハッシュ値に対応する公開鍵の集まりを得る（ステップ S902）。詳しくは、組み込み機能部 921 は、各ハッシュ値 92231 ~ 9223m を公開鍵 92221 ~ 9222m でそれぞれ復号してプログラム本体 9221 および公開鍵群 92221 ~ 9222m を組み合わせて作成されたデータをハッシングした各ダイジェストを得る一方、プログラム本体 9221 および公開鍵群 92221 ~ 9222m を組み合わせて作成されたデータを既知のハッシュ関数でハッシングしたダイジェストを得、両各ダイジェストが完全に一致するかどうかをそれぞれ検証することで、各ハッシュ値 92231 ~ 9223n がプログラム本体 9221 および公開鍵群 92221 ~ 9222n と各公開鍵 92221 ~ 9222n と対をなす各秘密鍵（図示せず）とによって生成されたものであることをそれぞれ確認し、確認したハッシュ値に対応する公開鍵の集まりを得る。すなわち、プログラム本体 9221 および公開鍵群 92221 ~ 9222m 中の少なくとも 1 つ以上の公開鍵が改竄されたものでなく、真正な出所由来をもつことを確認する。なお、この確認処理は、親機器 92 にプログラム 922 が導入、たとえばインストールされたときなどに 1 回行われればよい。

【0211】次に、携帯機器 91 内のプログラム 912 を実行するプロセス 9120 と親機器 92 内のプログラ

ム 9 2 2 を実行するプロセス 9 2 2 0 とが通信をしようとして通信要求が発生した場合 (ステップ S 9 0 3)、またはそれ以前に、まず、携帯機器 9 1 の組み込み機能部 9 1 1 と親機器 9 2 の組み込み機能部 9 2 1 との間で、携帯機器 9 1 に付随する秘密鍵 9 1 3 1 および公開鍵 9 1 3 2 と、親機器 9 2 に付随する秘密鍵 9 2 3 1 および公開鍵 9 2 3 2 とを用いた公開鍵方式により相互認証を行う (ステップ S 9 0 4)。

【0212】たとえば、親機器 9 2 は、自らが通信してよい相手を示す公開鍵として保持する携帯機器 9 1 に付随する公開鍵 9 1 3 2 と、携帯機器 9 1 が保持する携帯機器 9 1 に付随する公開鍵 9 1 1 3 2 とが一致するかどうかを判定し、一致した場合に携帯機器 9 1 の認証を行う。一方、携帯機器 9 1 は、自らが通信してよい相手を示す公開鍵として保持する親機器 9 2 に付随する公開鍵 9 2 3 2 と、親機器 9 2 が保持する親機器 9 2 に付随する公開鍵 9 2 1 3 2 とが一致するかどうかを判定し、一致した場合に親機器 9 2 の認証を行う。

【0213】また、RSA の公開鍵によるワン・タイム・パスワード方式を用いた場合、携帯機器 9 1 の組み込み機能部 9 1 1 は親機器 9 2 にランダムな文字列を送り (“Challenge”)、親機器 9 2 の組み込み機能部 9 2 1 はその文字列を親機器 9 2 に付随する秘密鍵 9 2 3 1 で暗号化して携帯機器 9 1 に送り返し (“Response”)、携帯機器 9 1 の組み込み機能部 9 1 1 は、暗号化した文字列を親機器 9 2 に付随する公開鍵 9 2 3 2 で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、親機器 9 2 を通信してよい相手 (つまり、親機器 9 2 に付随する公開鍵 9 2 3 2 と対をなす秘密鍵 9 2 3 1 を所有するもの) であると認証する。一方、親機器 9 2 の組み込み機能部 9 2 1 は携帯機器 9 1 にランダムな文字列を送り (“Challenge”)、携帯機器 9 1 の組み込み機能部 9 1 1 はその文字列を携帯機器 9 1 に付随する秘密鍵 9 1 3 1 で暗号化して親機器 9 2 に送り返し (“Response”)、親機器 9 2 の組み込み機能部 9 2 1 は暗号化した文字列を携帯機器 9 1 に付随する公開鍵 9 1 3 2 で復号し、復号した文字列と先に送ったランダムな文字列とが一致すれば、携帯機器 9 1 を通信してよい相手 (つまり、携帯機器 9 1 に付随する公開鍵 9 1 3 2 と対をなす秘密鍵 9 1 3 1 を所有するもの) であると認証する。

【0214】相互認証に成功した場合、携帯機器 9 1 の組み込み機能部 9 1 1 および親機器 9 2 の組み込み機能部 9 2 1 は、ハッシュ値確認結果の公開鍵の集まりをお互いに相手に伝え、一致する公開鍵があるかどうかを判定し (ステップ S 9 0 5)、一致する公開鍵が 1 つ以上ある場合に限り、プロセス 9 1 2 1 0 とプロセス 9 2 2 1 0 との間で通信を許可する (ステップ S 9 0 6)。

【0215】ステップ S 9 0 4 で携帯機器 9 1 または親機器 9 2 の相互認証に失敗した場合、またはステップ S

0 5 で一致する公開鍵が 1 つもなかった場合、携帯機器 9 1 の組み込み機能部 9 1 1 および親機器 9 2 の組み込み機能部 9 2 1 は、プロセス 9 1 2 0 とプロセス 9 2 2 0 との間の通信を不許可とする (ステップ S 9 0 7)。

【0216】なお、上記第 9 の実施の形態では、ステップ S 9 0 5 で携帯機器 9 1 によるハッシュ値確認結果の公開鍵の集まりと親機器 9 2 によるハッシュ値確認結果の公開鍵の集まりとに一致する公開鍵が 1 つ以上含まれていればプログラム 9 1 2 および 9 2 2 が真正な出所由来をもつものであると判定したが、携帯機器 9 1 によるハッシュ値確認結果の公開鍵の集まりと親機器 9 2 によるハッシュ値確認結果の公開鍵の集まりとの公開鍵がすべて一致したときにのみ、プロセス 9 1 2 1 0 とプロセス 9 2 2 1 0 との間で通信を許可するようにすることもできる。

【0217】第 9 の実施の形態によれば、プログラム 9 1 2 および 9 2 2 が該プログラム 9 1 2 および 9 2 2 の出所由来を表す公開鍵群 9 1 2 2 1 ~ 9 1 2 2 n および 9 2 2 2 1 ~ 9 2 2 2 n をもつことを許す場合はプログラム本体 9 1 2 1 および 9 2 2 1 とともに保持する公開鍵群 9 1 2 2 1 ~ 9 1 2 2 n および 9 2 2 2 1 ~ 9 2 2 2 n に対して署名群であるハッシュ値群 9 1 2 3 1 ~ 9 1 2 3 n および 9 2 2 3 1 ~ 9 2 2 3 n を付すことから、プログラム 5 1 2 および 5 2 2 の成りすましを防止することができる。

【0218】

【発明の効果】第 1 の効果は、外部装置が、盗み見や改竄が可能な環境下にあるプログラムを元にし動作する装置と通信を行う場合に、成りすましを防止しかつ通信相手のプログラムの認証を行うことができることである。その理由は、プログラムが秘密鍵をもたないで認証が可能だからである。

【0219】第 2 の効果は、プログラムが成りすましを防止しかつ複数の出所由来を表す公開鍵をもつことを許すことができることである。その理由は、複数の出所由来を表す公開鍵をもつことを許す場合は、プログラム本体とともに保持する公開鍵群に対し署名するからである。

【0220】第 3 の効果は、悪意のプログラムに対しセキュリティを保てることである。その理由は、プログラムの出所由来を表す ID、つまりプログラムの製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うからである。

【0221】第 4 の効果は、ユーザ管理のような集中管理システムを必要としない分散環境下での通信による処理についてのセキュリティを保てることである。その理由は、プログラムの出所由来を表す ID、つまりプログラムの製造元やバージョンに類する情報を元にしたアクセス制御により通信を行うため、悪意のプログラムに対しセキュリティを保てるからである。

【0222】第5の効果は、プログラム実行・通信装置内のプログラムのもつ情報の、流通する範囲が出所由来を同じくするプログラムの範囲内に限られることである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すIDを有するプログラムとしか通信できず、任意の他のプログラムと通信できないためである。

【0223】第6の効果は、プログラム実行・通信装置内のプログラムのもつ情報が、たとえプログラムが暴走しても、出所由来を同じくするプログラムの範囲外に漏洩しないことである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すIDを有するプログラムとしか通信できず、任意の他のプログラムと通信できないためである。

【0224】第7の効果は、プログラム実行・通信装置内のプログラムのもつ情報の、流通する範囲が、出所由来を同じくするプログラムの範囲内に限られることである。その理由は、プログラム実行・通信装置内のプログラムが、一致する出所由来を表すIDを公開鍵とすることにより、同じ秘密鍵を保持するものにより提供されたプログラムの間でしか、通信ができないからである。

【0225】第8の効果は、分散環境における通信範囲の制御についてのセキュリティ面での設計が容易になり、かつ自由度が変わらないことである。その理由は、分散環境におけるもっとも重要な問題の1つである通信時の情報漏洩について、出所由来を同じくするプログラムの間でしか情報を流通させないために、設計時に情報の流通範囲を設計しなくても、悪意のある他者への漏洩や、プログラムのバグ、暴走による漏洩が起らず、また、逆に1つのサービスにおいては、そのプロジェクトにかかわるもの全体である1つの製造元またはそれに類するものとみなすことで、情報の流通を行え、またその流通範囲で十分であるからである。

【0226】第9の効果は、悪意のプログラムに対しセキュリティを保てることである。その理由は、プログラムの出所由来を表すID、つまりプログラムの製造元やバージョンに類する情報を元に通信可否を行うからである。

【0227】第10の効果は、ユーザ管理のような集中管理システムを必要としない分散環境下での通信による処理についてのセキュリティを保てることである。その理由は、プログラムの出所由来を表すID、つまりプログラムの製造元やバージョンに類する情報を元に通信可否を行うため、悪意のプログラムに対しセキュリティを保てるからである。

【0228】第11の効果は、公開鍵別の通信を行う場合に、通信路に関するシステム設計が容易であることである。その理由は、どの通信路がどの公開鍵用で占有されるかが予め限定されているからである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの構成を示すブロック図である。

【図2】第1の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの処理を示す流れ図である。

【図3】本発明の第2の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの構成を示すブロック図である。

【図4】第2の実施の形態に係る秘密鍵なしプログラム認証方法が適用された情報システムの処理を示す流れ図である。

【図5】本発明の第3の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図6】第3の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図7】本発明の第4の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図8】第4の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図9】本発明の第5の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの構成を示すブロック図である。

【図10】第5の実施の形態に係るプログラムID通信処理制御方法が適用された情報システムの処理を示す流れ図である。

【図11】本発明の第6の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図12】第6の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

【図13】本発明の第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図14】第7の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

【図15】本発明の第8の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの構成を示すブロック図である。

【図16】第8の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

【図17】本発明の第9の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの構成

を示すブロック図である。

【図18】第9の実施の形態に係るプログラムID通信範囲制御方法が適用された情報システムの処理を示す流れ図である。

【図19】従来の情報システムの構成の一例を説明するブロック図である。

【図20】従来の情報システムの構成の他の例を説明するブロック図である。

【図21】従来の情報システムの構成の別の例を説明するブロック図である。

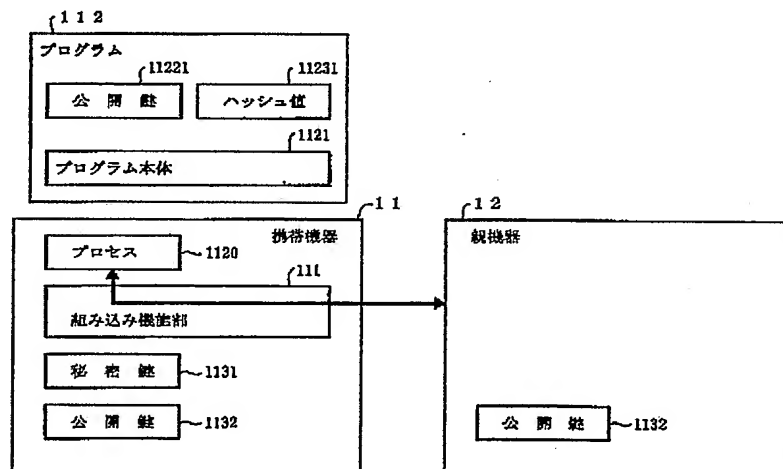
【符号の説明】

11, ..., 91 携帯機器
 12, ..., 92 親機器
 111, ..., 911 組み込み機能部
 112, ..., 912 プログラム
 1120, ..., 9120 プロセス
 1121, ..., 9121 プログラム本体
 11221~1122n, ..., 91221~9122n
 公開鍵
 11231~1123n, ..., 91231~9123n 20
 ハッシュ値
 11241~1124n, ..., 91241~9124n
 秘密鍵
 1131, ..., 9131 秘密鍵
 1132, ..., 9132 公開鍵
 81511~8151i, 82511~8251j 仮想ソケット
 81521~8152k, 82521~8252l ソ

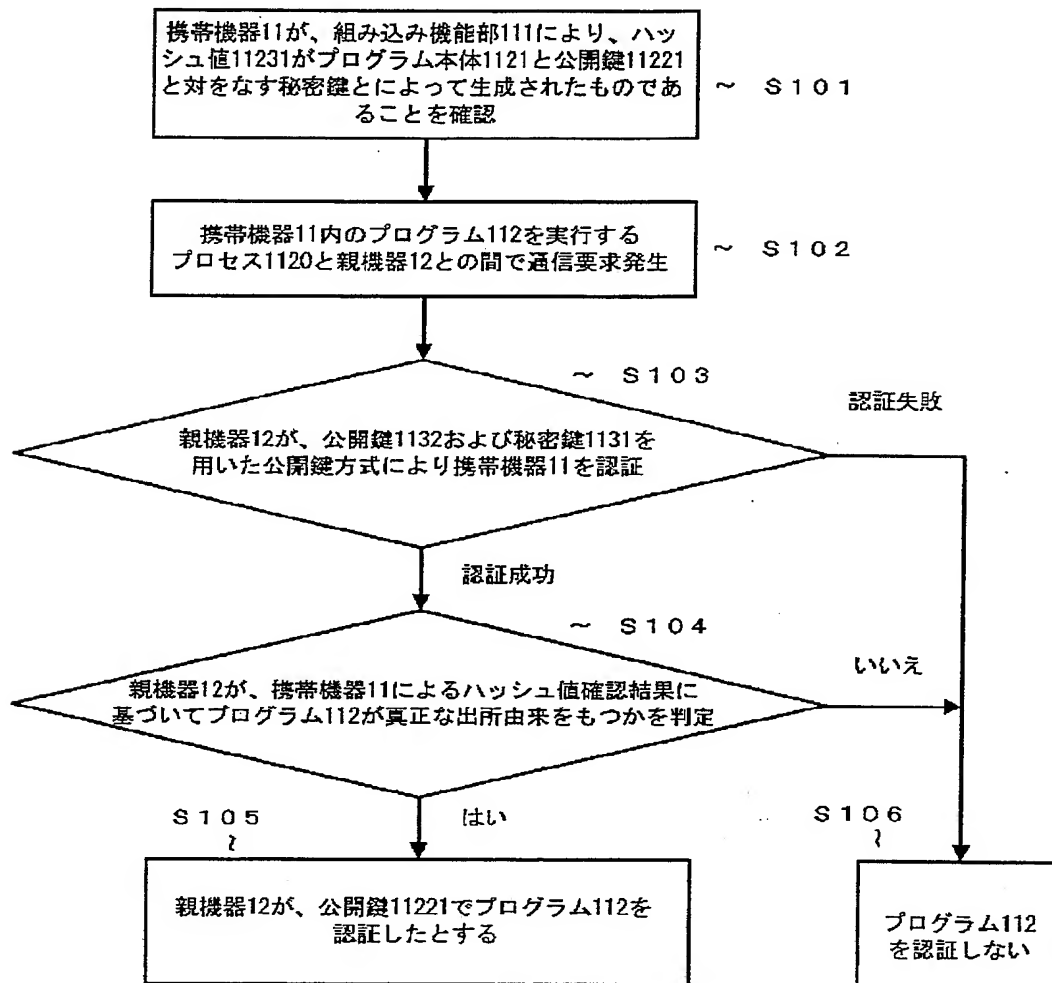
ケット

S101, S201, S401, S501, S701,
 S702, S801, S802, S901, S902
 ハッシュ値確認ステップ
 S102, S202, S301, S402, S502,
 S601, S703, S803, S903 通信要求発生ステップ
 S103, S203, S403, S503 携帯機器認証ステップ
 10 S104, S204, S404, S504 プログラム出所由来判定ステップ
 S105, S205, S303 プログラム認証ステップ
 S106, S206 プログラム不認証ステップ
 S302, S602 公開鍵獲得ステップ
 S304, S405, S505 通信・処理ステップ
 S305, S406, S506 通信・処理なしステップ
 S603, S704 相互認証ステップ
 S604 公開鍵比較ステップ
 S605 相互認証・公開鍵一致判定ステップ
 S606, S706, S806, S906 通信許可ステップ
 S607, S707, S807, S907 通信不許可ステップ
 S705, S805, S905 公開鍵一致判定ステップ
 S804, S904 相互認証ステップ

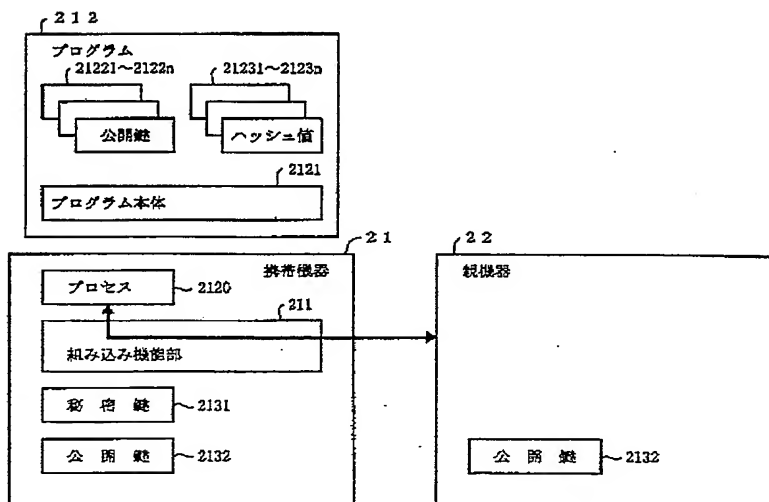
【図1】



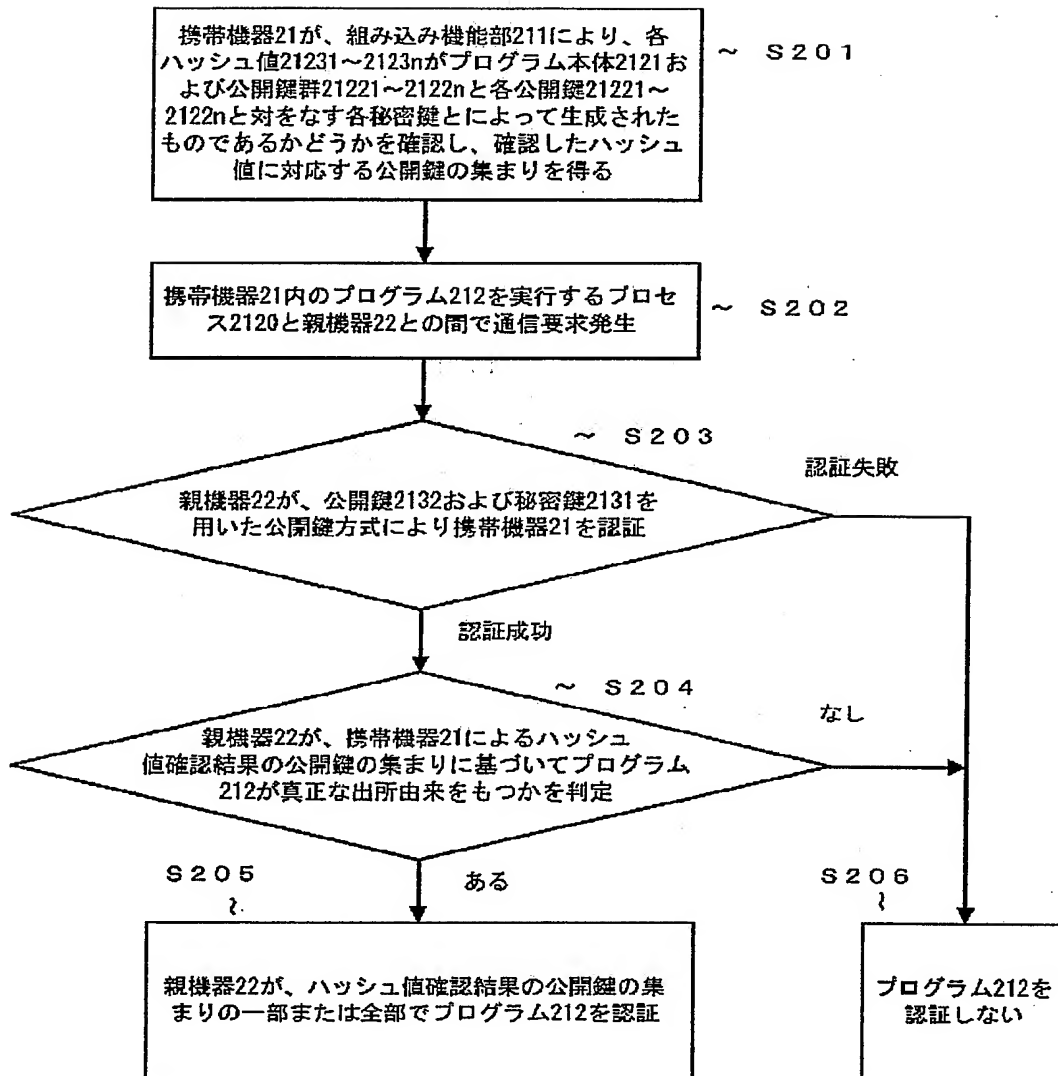
【図 2】



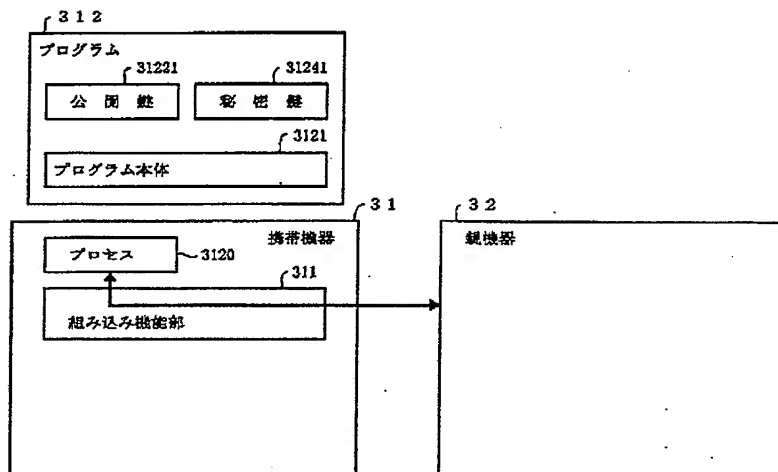
【図 3】



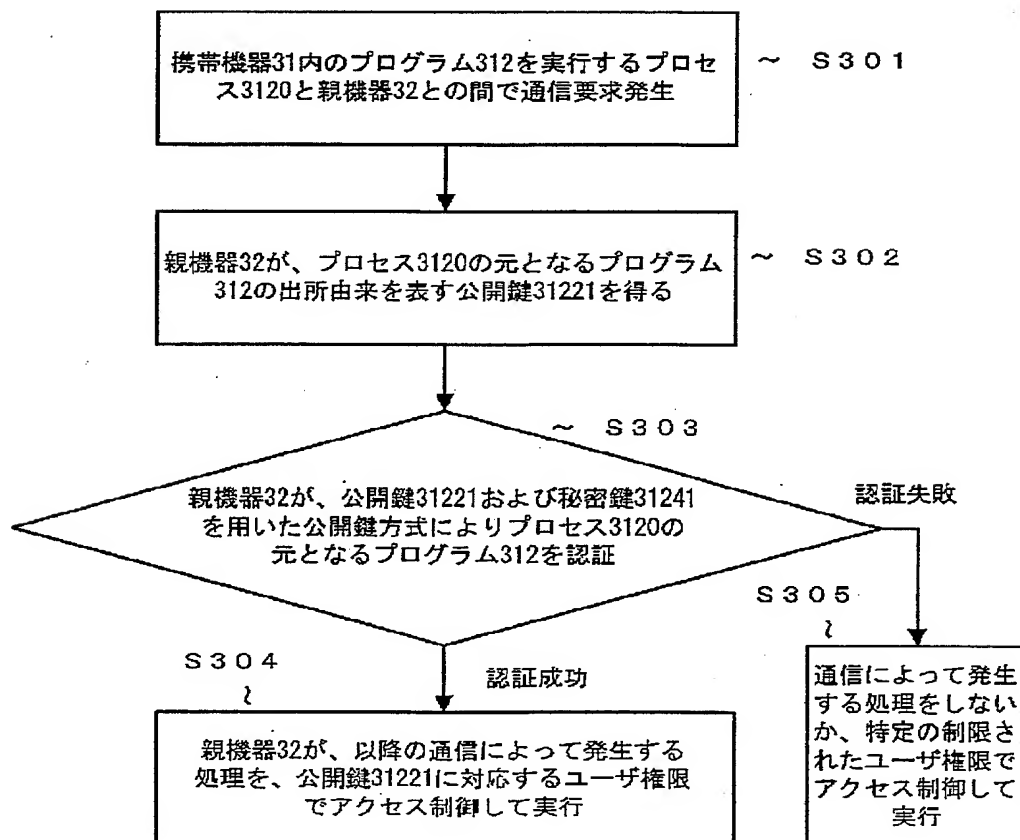
【図 4】



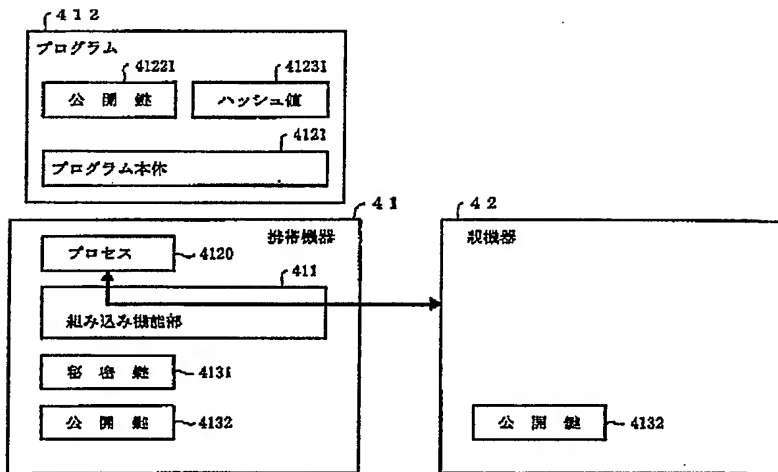
【図 5】



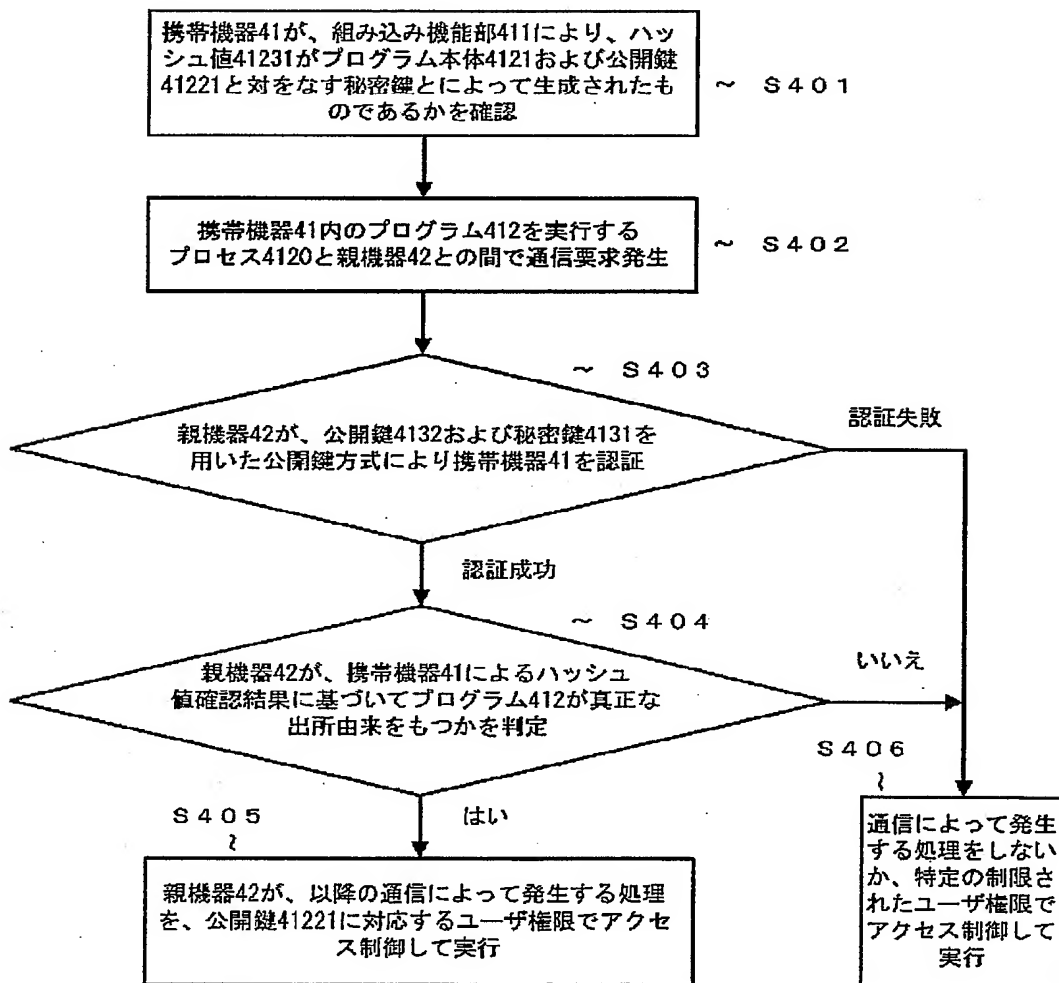
【図 6】



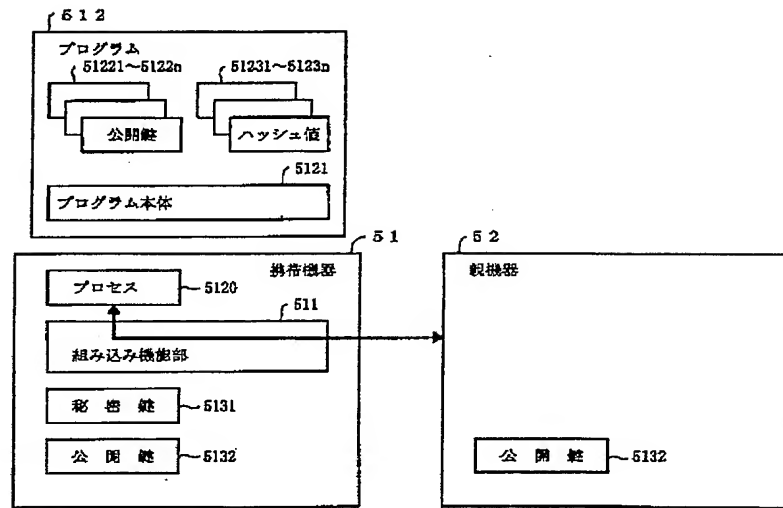
【図 7】



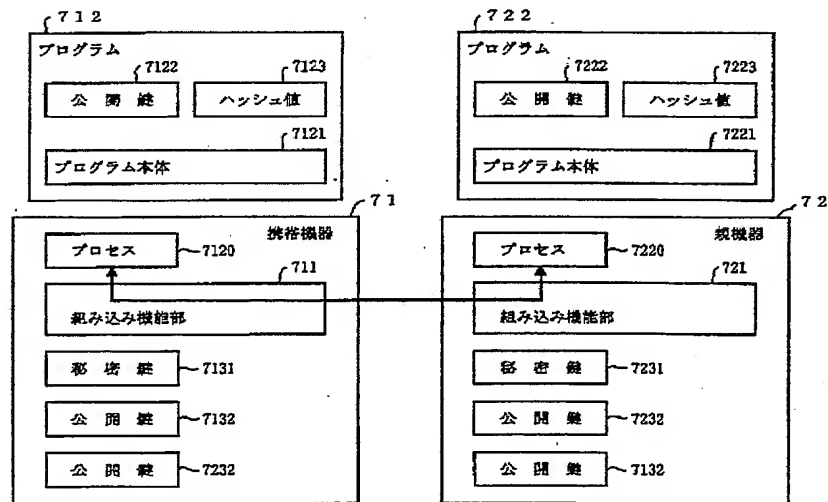
【図 8】



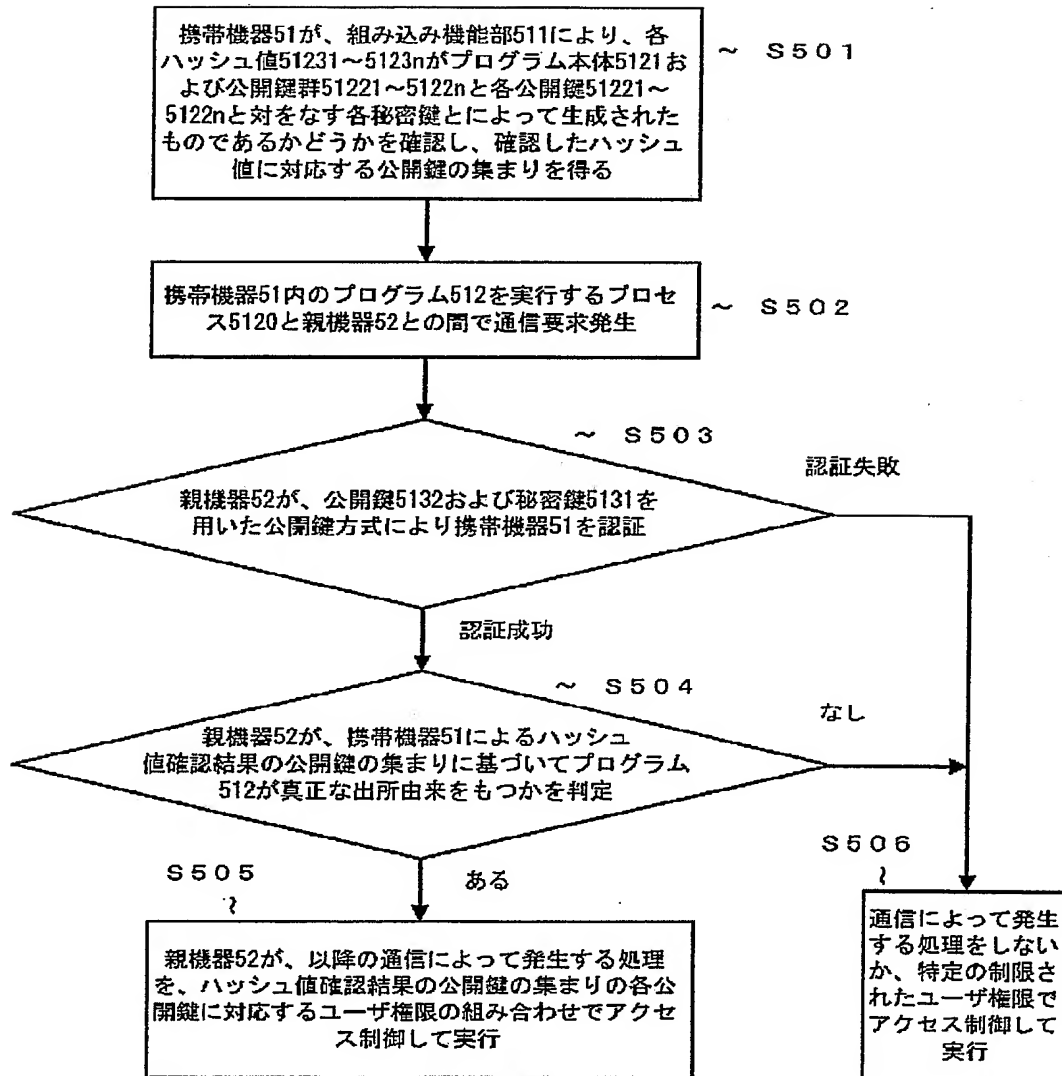
【図 9】



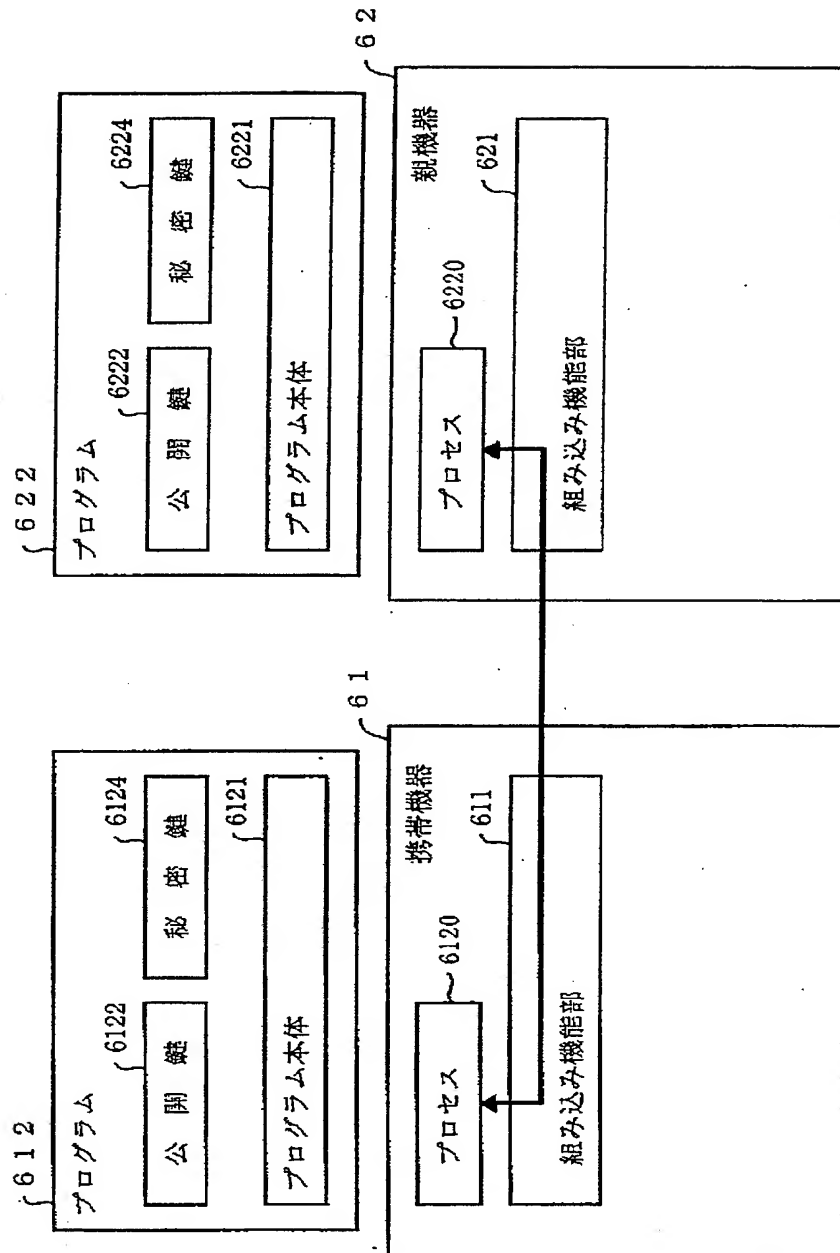
【図 13】



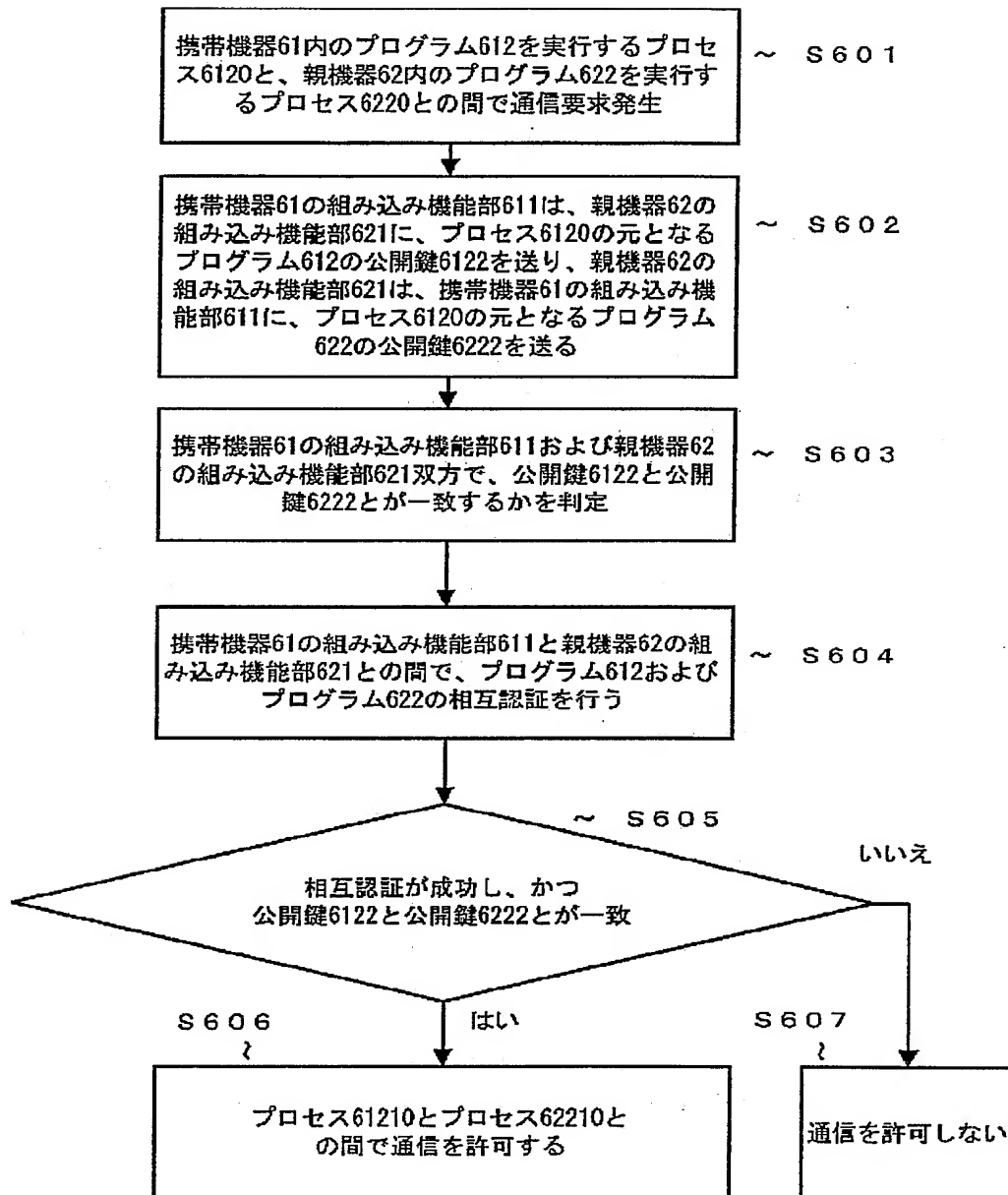
【図 10】



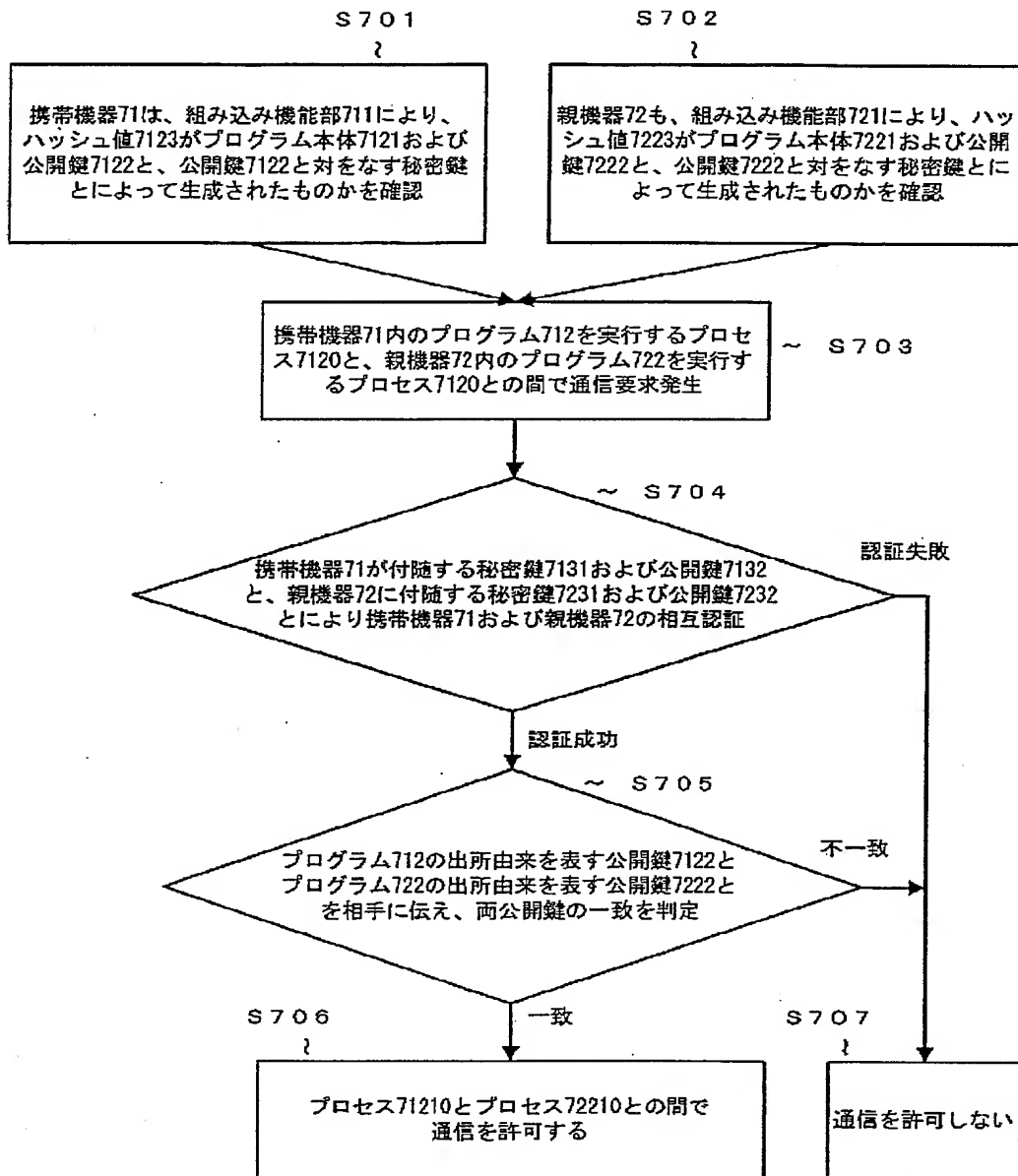
【図 11】



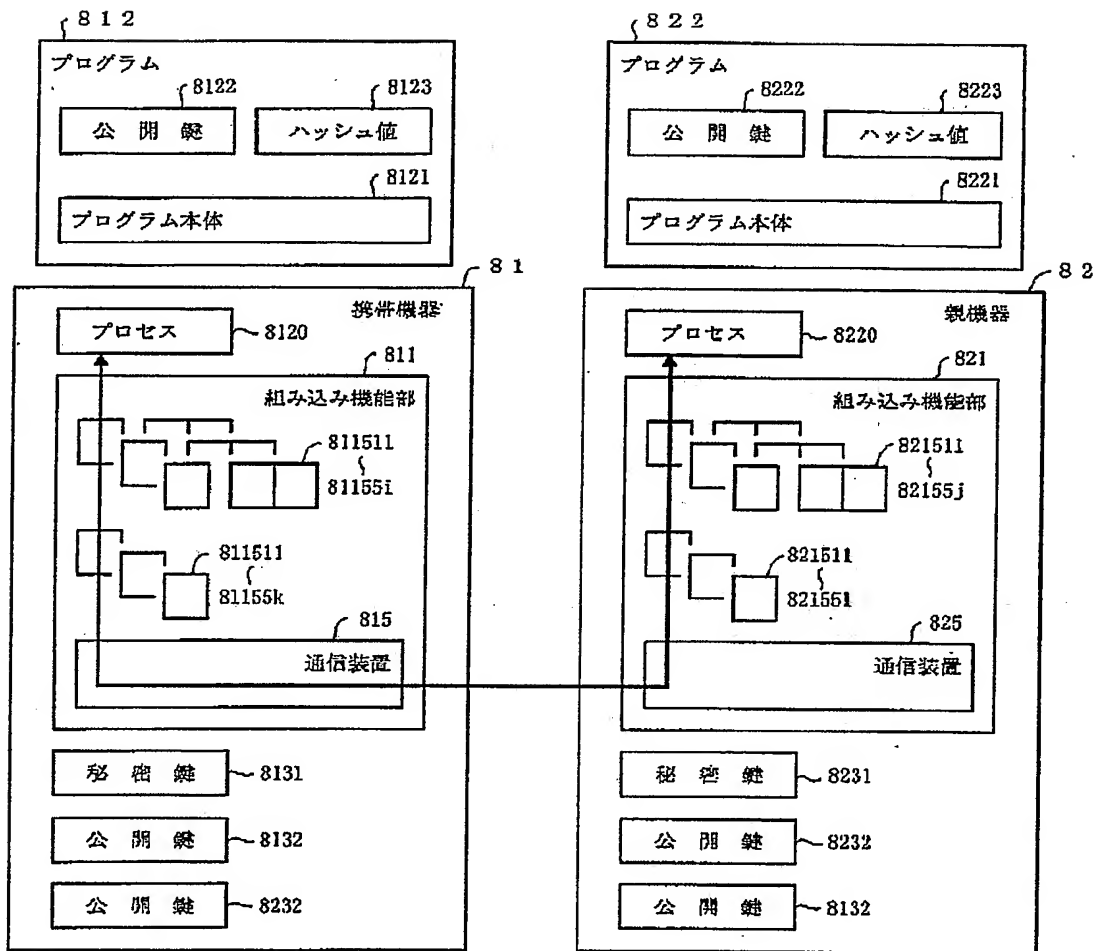
【図 12】



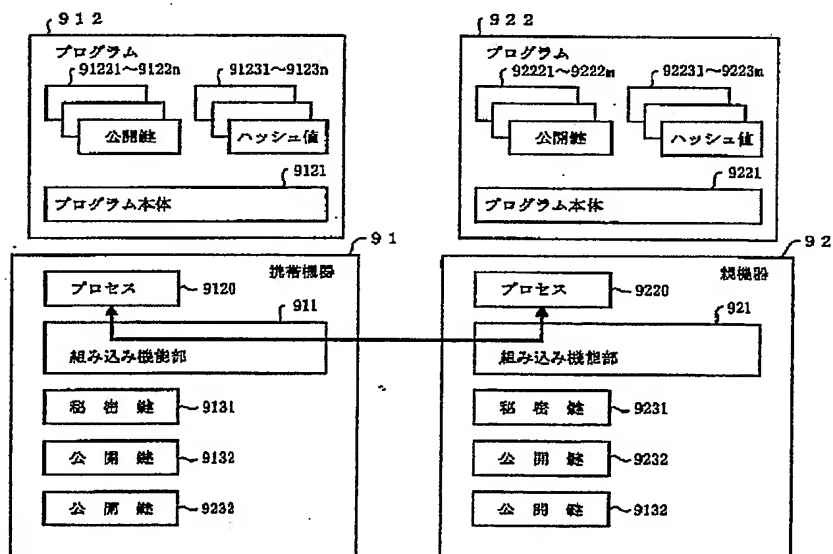
【図 14】



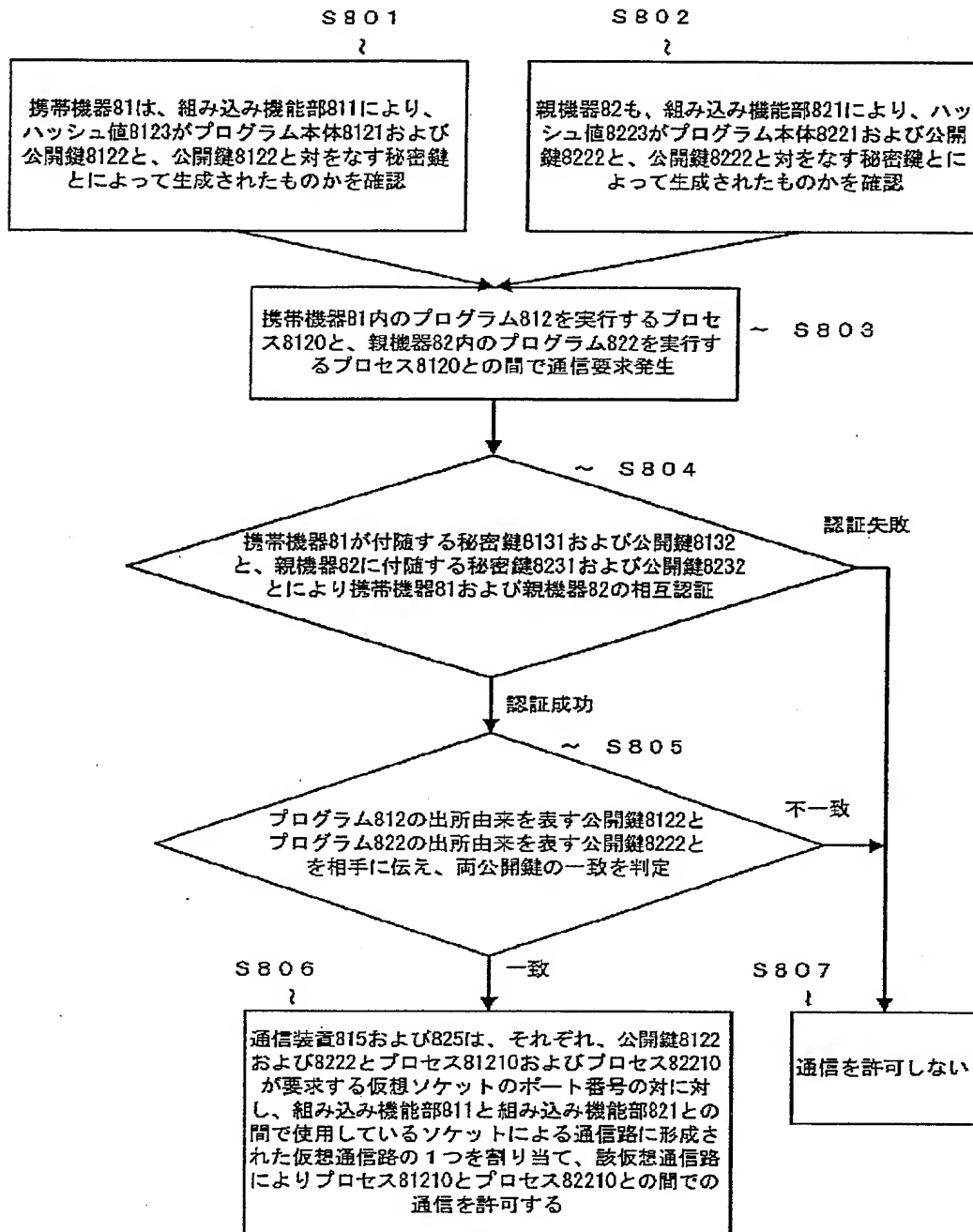
【図 15】



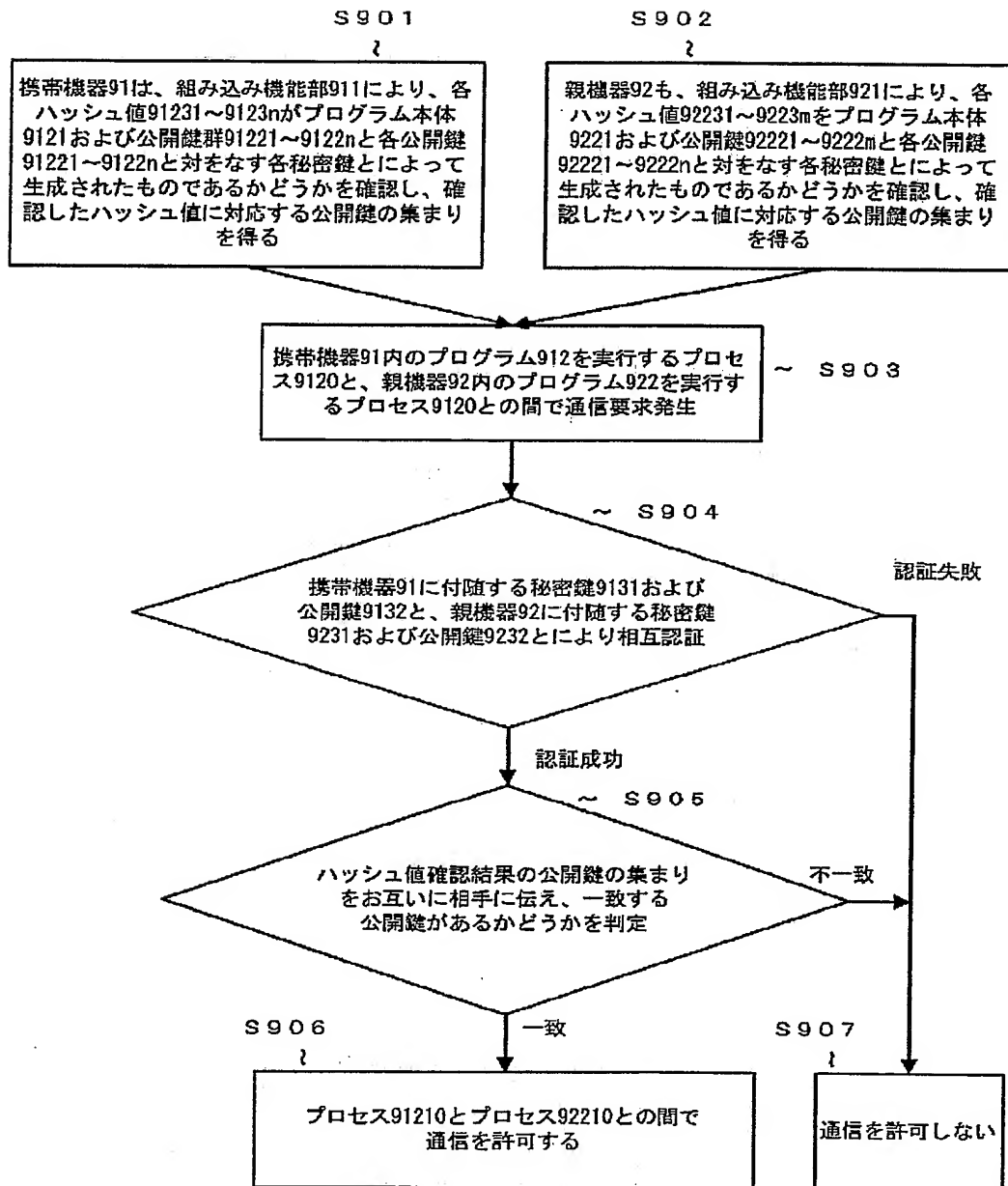
【図 17】



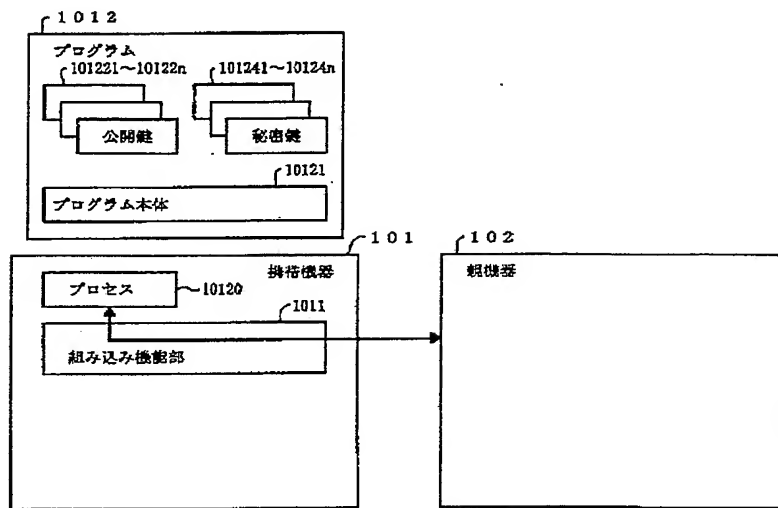
【図 16】



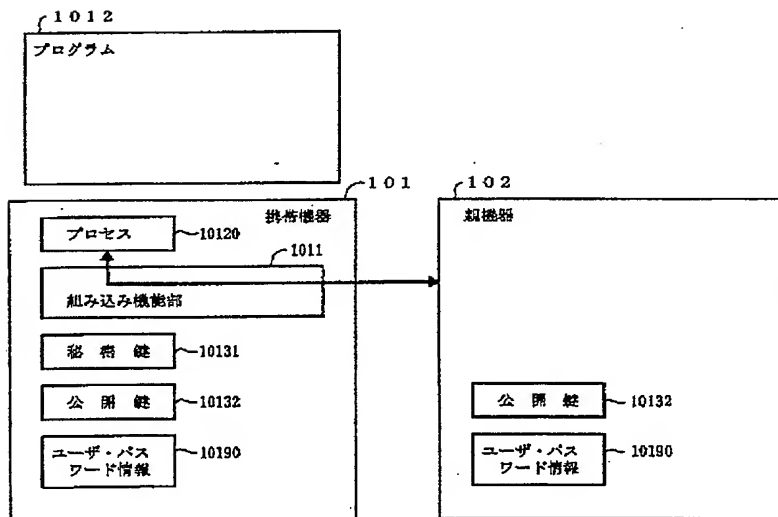
【図18】



【図 19】



【図 20】



【図 21】

